



**Interpretive Letter #1175
December 2020**

November 16, 2020

Subject: Customer Identification Program Rule Exemption Request for [**OpSub**], an Operating Subsidiary of [**Bank**]

Dear []:

I am writing in response to your letter (request letter) dated February 14, 2020, on behalf of [**Bank**] ([**Bank**] or Bank) regarding the application of the Bank Secrecy Act to its operating subsidiary, [**OpSub**], an online payment service provider or payment gateway.¹ Your letter requested, among other things, a legal interpretation that addresses whether the service [**OpSub**] provides to customers meets the definition of an “account” for purposes of the customer identification program (CIP) rule, 31 C.F.R. § 1020.220 and, if there is an account, a limited exemption from the requirements of the CIP rule to permit [**OpSub**]’s proposed onboarding process. Specifically, [**OpSub**] proposed to onboard certain parties by collecting partial tax identification numbers (TINs) directly and only obtain the full TIN during the verification process from a trusted third-party source (e.g., LexisNexis, credit reporting agency). Consistent with 12 C.F.R. § 5.34, which generally provides that operating subsidiaries of national banks conduct activities pursuant to the same terms and conditions that apply to the conduct of such activities by its parent national bank, we conclude that certain services provided by [**OpSub**] result in the establishment of an “account” for purposes of the CIP rule because the same services provided by [**the Bank**] would result in the establishment of an account under the CIP rule. We also conclude that there is a valid basis for the requested exemption from the requirements of the CIP rule, and we hereby grant the exemption under the OCC’s Title 12 authority as published OCC policy that specifically addresses the activities of an operating subsidiary of a national bank.

¹ The Bank’s request revised and replaced a substantially similar request previously submitted by the Bank on January 10, 2019, as supplemented with responses to a request for additional information, which were received on April 17, 2019.

I. Background

A [**OpSub**] transaction involves four parties: (1) a payment portal website or the front-end processor (Platform Partner),² (2) an individual or entity (e.g., business, contractor, [] []) that receives a payment (Payee), (3) an individual or entity transferring money to the Payee in return for services provided (Payor), and (4) an acquiring bank, which is [**the Bank**]. [**OpSub**] facilitates a payment transaction between the Payor and Payee by providing the technological means to capture payments instructions provided by the two parties to the Platform Partner (e.g., a [] website or accounting and billing software) and transferring instructions to [**the Bank**] to process and facilitate the transfer of funds between the parties through their financial institutions.

Specifically, [**OpSub**] allows Platform Partners to integrate their websites into [**OpSub**]'s Application Program Interface (API) in order to provide Platform Partners with access to services, including their payment checkout process, which includes payment initiation and processing and access to a pooled account at [**the Bank**]. [**OpSub**]'s API enables these transactions by transferring payment information (i.e., payment messages or instructions) from the Payor's financial institution (e.g., a credit/debit card issuing bank) to [**the Bank**], which uses the instructions to process the payments by drawing funds from the Payor's financial institution, placing the funds into a pooled account at [**the Bank**] that is established for the benefit of the Payees, and subsequently settles the payment by moving the funds from the pooled account to the Payee's demand deposit account (DDA).³ Currently, [**OpSub**] treats the Platform Partner and the Payees, but not the Payor, as customers for purposes of the CIP rule.

The only payment methods that are supported by [**OpSub**] are debit cards, credit cards, prepaid cards, gift cards, and automated clearing house (ACH) transfers, products that can only be provided by regulated financial institutions subject to the Bank Secrecy Act (BSA) or other anti-money laundering (AML) laws.⁴ The Payees are required, by contract or as a matter of practice, to have a DDA with a U.S. regulated financial institution into which all transactions are settled

² These are independent websites and businesses that provide business, [] including book-keeping, invoicing, and registration and payments services. [**OpSub**]'s Platform Partners generally fall into two categories: (1) [] websites []

[] and (2) integrated software vendors that sell business-related software to small and medium businesses (e.g., accounting and billing software that integrates a payment function via [**OpSub**]).

³ The [**Terms of the Agreement**] provide that the pooled account is established in the name of [**the Bank**] for the benefit of the Payees and other users. []

[]. As part of the process, [**OpSub**] collects, analyzes, and relays to [**the Bank**] payments information generated between a Payor and Payee using the Platform Partner. [**OpSub**] does not have any legal or constructive ownership or control over the funds, nor does it transmit money or monetary value. [**The Bank**] has represented that [**OpSub**] is not a money service business and is not required to register with FinCEN.

⁴ [**OpSub**] supports "most domestic and international" credit, debit, prepaid, or gift cards with a Visa, Mastercard, American Express, or Discover logo. Payments via ACH are only permitted from U.S.-based Payors with a U.S. bank account to a U.S.-based Payees. []

by **[the Bank]**.⁵ Furthermore, Payees must be either a U.S. citizen, legal permanent resident of the United States, or a U.S. business or nonprofit organization having a physical presence in the United States and authorized to conduct business by the state in which it operates.⁶ Thus, on the Payee side of the payment transaction, CIP is conducted and other BSA/AML processes are applied when the Payee establishes a DDA with a financial institution in the United States. There is no CIP review of Payors by **[OpSub]/[the Bank]** since such parties are not “customers” of **[OpSub]/[the Bank]** for CIP purposes. There, however, will be some level of BSA/AML identification, due diligence, and monitoring processes applied to such Payors by another financial institution depending on the payment method at issue.⁷

II. Proposed Onboarding Process

On February 14, 2020, **[the Bank]** submitted the request letter, seeking an alternative onboarding process with respect to these parties. As explained in the request letter, the Bank requested an exemption from the requirements of 31 C.F.R. § 1020.220(a)(2)(i)(A)(4) to allow **[OpSub]** to onboard parties it has identified as customers for purposes of the CIP rule (customers) by collecting the last four digits of the TIN directly from the party and obtaining the full TINs from a third-party source during the verification process. If the customer fails verification either because there is a discrepancy between the partial TIN provided by the customer and the full TIN obtained from the third-party source, or the full TIN cannot be collected from a third-party source, **[OpSub]** would perform a manual verification process by requesting the full TIN directly from the customer to perform verification. **[OpSub]** would resolve any discrepancy to its satisfaction before the customer is onboarded.

The request letter represents that the modified CIP process meets “the spirit and purpose of existing BSA/AML regulations,” and poses a low risk of money laundering. The request letter contends that this modified CIP process allows **[OpSub]** to form a reasonable belief that it knows

⁵ Prior to April 1, 2019, **[OpSub]**’s **[Terms of the Agreement]** explicitly required entities establishing a **[OpSub]** “Account” to have a verified “U.S. banking account” to settle funds. The current **[Terms of the Agreement]** no longer expressly require settlement to a U.S. banking account, or a banking account at all, since settlement can be made to “other payment instruments.” Notwithstanding this change in the **[Terms of the Agreement]**, **[the Bank]** represents that currently it still requires a U.S. bank account to establish a **[OpSub]** account in the ordinary course. The Bank further represented that the change reflected that (1) a small number of its merchant clients settle by paper check ([]%), and (2) **[OpSub]** may accept other forms of settlement in the future, such as settlement to a prepaid card. The exemption is being granted on the condition that **[the Bank]** continues its practice of requiring Payees establishing a **[OpSub]** “Account” to have a verified “U.S. banking account” to settle funds.

⁶ [] (“**[OpSub]** allows businesses (including sole proprietorships), non-profit organizations and other entities to register for **[OpSub]** if they are located in one of the 50 United States or the District of Columbia . . . A Merchant must be either a United States citizen, a legal permanent resident of the United States, or a United States business or nonprofit organization having a physical presence in the United States and authorized to conduct business by the state in which it operates.”). In contrast, Payors may be foreign entities or individuals.

⁷ The CIP exemption discussed in this letter does not alter in any way **[Bank]/[OpSub]**’s BSA/AML obligations with respect to Payors because, as discussed in greater detail below, they are not **[the Bank]/ [OpSub]** customers. The exemption discussed in this letter therefore does not change the status quo for how such parties are permitted to access **[OpSub]**’s service.

the true identify of its customer. In support of this contention, the Bank notes that **[OpSub]** would continue to collect three of the four pieces of identifying information required under the CIP rules – name, address, and date of birth – directly from its customers. The only deviation with the proposed CIP process is the incomplete collection of TINs from its customers, which is promptly verified from a third-party source. The request letter also notes that **[OpSub]**'s practice of collecting partial TINs is similar to, but more limited than, the existing exemption available to the processing of credit card accounts, which permits the collection of *all* identifying information from a third-party instead of directly from the customer.⁸ The rationale supporting the credit card exemption was that the credit card industry's practices of obtaining "some information from the customer opening a credit card account, and the remaining information from a third-party source, such as a credit reporting agency, prior to extending credit to a customer . . . have produced an efficient and effective means of extending credit with little risk that the lender does not know the identity of the borrower."⁹ The request letter argues that this rationale should also apply to **[OpSub]**'s practice of collecting partial TINs.¹⁰

In addition, the request letter indicates that **[OpSub]**'s services present a low risk of money laundering because the forms of payment accepted are products that are generally provided by regulated financial institutions, which means Payors are generally subject to the BSA or some level of AML requirements. Payees are generally subject to BSA requirements by U.S. regulated financial institutions that maintain the Payee's U.S. DDA into which all transactions are settled. Therefore, the request letter maintains that on both sides of the payment transaction, each party is subject to some level of BSA or AML requirements, or both, by regulated financial institutions.

Moreover, the request letter maintains that this modified CIP process is consistent with fintech industry standards, balances its customers' privacy concerns in providing sensitive personal identification information through the Internet, and, because **[OpSub]** onboards customers in part through third-party platforms that have adopted these industry standards, other third-party web-based platforms may be reluctant to modify their systems to accommodate **[OpSub]**.

III. Legal Analysis

a. Applicability of the CIP Rule to Operating Subsidiaries of National Banks

As noted above, the CIP rule applies to "banks," as defined in the Bank Secrecy Act regulations at 31 C.F.R. § 1020.100(b), which does not include non-bank subsidiaries. Accordingly, the CIP regulation does not directly apply to **[OpSub]**. Instead, **[OpSub]** is subject to the CIP rule indirectly through the regulations issued under the National Bank Act because it is an operating

⁸ 31 C.F.R. § 1020.220(a)(2)(i)(C).

⁹ 68 Fed. Reg. 25,090, 25,097 (May 9, 2003).

¹⁰ The request letter represents that customers are reluctant to provide full TIN (SSN) because of privacy and fraud concerns raised with respect to the Internet. In addition, the request letter indicates that requiring **[OpSub]** to collect the full TIN directly from its customers would significantly impact its business by imposing more burdensome requirements on it relative to its competitors and by causing it to incur the significant time and expense of building such additional functionality into its system.

subsidiary of the Bank under 12 C.F.R. § 5.34, which provides that an “operating subsidiary conducts activities . . . pursuant to the same authorization, terms and conditions that apply to the conduct of such activities by its parent national bank, unless otherwise specifically provided by statute, regulation, or published OCC policy” This requirement to conduct business pursuant to the same authorization and conditions that apply to the parent national bank is consistent with the OCC’s view regarding the authority to establish an operating subsidiary as “incidental” to the business of banking. If a national bank has authority to conduct an activity as part of the business of banking, it is “incidental” to the business of banking to engage in the activity through an operating subsidiary under the same conditions and restrictions.¹¹

To date, the OCC has only issued a limited number of exemptions from the requirements of the CIP rule and none of which applied only to operating subsidiaries under 12 C.F.R. § 5.34.¹² Accordingly, the OCC has not previously articulated how the exemption procedures in 31 C.F.R. § 1020.220(b) apply in the context of a national bank operating subsidiary under 12 C.F.R. § 5.34. In order to ensure that operating subsidiaries continue to operate subject to the same terms and conditions as would apply to the parent bank, the OCC will apply the exemption standard in 31 C.F.R. § 1020.220(b) to operating subsidiaries under 12 C.F.R. § 5.34. In applying this exemption standard, the OCC will notify FinCEN and will consider any comments offered by FinCEN (though a formal FinCEN concurrence will not be required as under the CIP rule).¹³

b. CIP Rule Overview

Under the CIP rule, banks are required to implement a CIP that includes risk-based verification procedures that enable the bank to form a reasonable belief that it knows the true identity of its customers.¹⁴ These procedures must specify the identifying information that a bank will obtain

¹¹ See OCC Interpretive Ruling § 7.10, 31 Fed. Reg. 11459, 11460 (August 31, 1966) (“Therefore, this Office has concluded that the authority of a national bank to purchase or otherwise acquire and hold stock of a subsidiary operations corporation may properly be found among ‘such incidental powers’ of the bank ‘as shall be necessary to carry on the business of banking,’ within the meaning of [12 U.S.C. § 24(7)], or as an incident to another Federal banking statute which empowers a national bank to engage in a particular function or activity.”). See also 12 C.F.R. § 5.34.

¹² See OCC Bulletin 2020-88, Revised Order Granting Exemption From Customer Identification Program Requirements for Premium Finance Lending (Oct. 9, 2020). The prior order applied to activities that could be performed by banks and their subsidiaries, including operating subsidiaries. In contrast, this interpretive letter is granting an exemption not to activities by a range of entities but to a specific operating subsidiary of a national bank.

¹³ The OCC is granting this exemption from the requirements of the BSA under the specific authority set forth in 12 C.F.R. § 5.34. An operating subsidiary of a national bank is not defined as a “financial institution” or as a “bank” that is subject to the requirements of the BSA. See 31 C.F.R. § 1010.100(t) (“financial institution”) and 1020.100(b) (“bank”). As a result, FinCEN concurrence is not required.

¹⁴ 31 C.F.R. § 1020.220(a)(2).

from each customer¹⁵ prior to opening an account,¹⁶ which at a minimum must include the customer's name, date of birth (for an individual), address, and identification number.¹⁷ The identification number must be a TIN for a U.S. person.¹⁸ For a non-U.S. person, one or more of the following is required: a TIN, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.¹⁹ The CIP must also contain procedures for verifying the identity of the customer.²⁰

Under 31 C.F.R. § 1020.220(b), the appropriate Federal functional regulator with the concurrence of the Secretary of the Treasury may by order or regulation exempt any bank or type of account from the requirements of the CIP rules. The Secretary's authority under this provision has been delegated to FinCEN. The Federal functional regulator and FinCEN must consider whether the proposed exemption would be consistent with the purposes of the BSA²¹ and safe and sound banking practices and may consider other appropriate factors.

c. Determining the Existence of an "Account" and Identifying the Customer

As previously noted, operating subsidiaries of national banks conduct activities pursuant to the same terms and conditions that apply to the conduct of such activities by its parent national bank, unless otherwise specifically provided by statute, regulation, or published OCC policy. The CIP rule requires risk-based procedures for verifying the identity of each "customer" opening a new "account" to the extent reasonable and practicable, that include, among other things, "procedures for opening an account that specify the identifying information that will be obtained *from each customer.*"²² Accordingly, in order to determine the application of the CIP rule, it is first essential to determine whether there is an "account" and, if so, which parties constitute the "customer" for purposes of the account. The FBAs and FinCEN issued an FAQ exempting data processing, data transmission, and data warehousing from the definition of "account" except for

¹⁵ 31 C.F.R. § 1020.100(c). A customer generally means a person that opens a new account.

¹⁶ 31 C.F.R. § 1020.100(a)(1). An account generally refers to "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit."

¹⁷ 31 C.F.R. § 1020.220(a)(2)(i)(A).

¹⁸ 31 C.F.R. § 1020.220(a)(2)(i)(A)(4)(i).

¹⁹ 31 C.F.R. § 1020.220(a)(2)(i)(A)(4)(ii).

²⁰ 31 C.F.R. § 1020.220(a)(2)(ii).

²¹ 31 U.S.C. § 5311 (setting forth the purposes of the BSA).

²² See 31 C.F.R. § 1020.220(a)(2)(i)(a). Under the CIP rule, an "account" generally refers to "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit." 31 C.F.R. § 1020.100(a)(1). The definition goes on to provide that an account does not include "a product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of check or money order." 31 C.F.R. § 1020.100(a)(2). A "customer" generally means "a person that opens a new account." 31 C.F.R. § 1020.100(c).

when they are established as part of a formal banking relationship.²³ To verify the identity of the person opening the account, the final CIP rule’s preamble explains that a bank generally need only verify the identity of the named accountholder.²⁴

In applying these principles, there are three potential categories of customers to consider for purposes of determining the application of the CIP rule under the **[OpSub]** framework. These potential customers are the Platform Partners, the Payees, and the Payors. As discussed below, **[OpSub]**’s CIP policies and procedures should be applied to the Platform Partners and the Payees. CIP does not apply to the Payors since there is no “account” or “customer” relationship.

Platform Partners

Generally, when processors establish a pooled account with a bank to process payments, the pooled account constitutes an “account” for purposes of the CIP rule and the customer is the processor that opens the account with a bank. In this context, the Platform Partner’s limited role of transferring data to facilitate transactions could be viewed as outside the scope of the CIP rule as a mere “data transmission” service. However, the exemption in the FAQ only applies to the underlying customers of these processors, and CIP continues to apply to the processing customer (generally a merchant) that opens a pooled account for the processing of payments since the pooled account is established as part of a formal banking relationship between the bank and the merchant processor.

Here, the **[OpSub]** package of services includes an “account” for CIP purposes, since there is a formal banking relationship established on behalf of the **[OpSub]** parties and funds are ultimately deposited into a pooled demand deposit account at the Bank for the purpose of processing payments. The Platform Partners are customers of **[OpSub]** for purposes of this account because they offer a bundle of services that includes the incidental processing of payments through the pooled account established at the Bank by **[OpSub]** for their benefit.²⁵

The Payees

The Payees are independent business customers of the Platform Partners, which establish a contractual relationship with **[OpSub]** and the Bank in order to receive payments from Payors. Banks generally are not required to “look through” to obtain CIP information from parties having

²³ FinCEN et al., FAQs: Final CIP Rule (Apr. 28, 2005), available at <https://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-16.html> (“Data processing, warehousing, and transmission services generally do not involve a service, dealing, or financial transaction that, taken alone, constitutes a ‘formal banking relationship’ within the meaning of 31 C.F.R. § 103.121(a)(1). If, however, any of these services are part of the establishment of a formal banking relationship, then the CIP rule in 31 C.F.R. § 103.121 would apply.”) The provisions in the former 31 C.F.R. Part 103 are found in 31 C.F.R. Parts 1000-1099 (Chapter X). See 75 Fed. Reg. 65,806 (Oct. 26, 2010).

²⁴ 68 Fed. Reg. 25,090, 25,094 (May 9, 2003).

²⁵ The account at the Bank is established in the Bank’s name for the benefit of the payees and platform partners and other users. See *supra* note 3.

rights against the entity opening a pooled account for purposes of payment processing.²⁶ This is because banks typically are expected to perform CIP and other due diligence procedures for the processing customers opening the pooled account and are generally not expected to obtain information from a customer's customer.²⁷ Despite this general rule, the Federal banking agencies and FinCEN have determined that in certain situations banks should "look through" pooled accounts to identify an individual or entity utilizing the account as a customer for purposes of CIP in certain circumstances.²⁸

Here, the OCC has determined that a similar analysis should be applied to the pooled accounts to identify Payees as a customer for purposes of CIP even if such Payees are not named accountholders under the pooled account. Payees are independent businesses that offer various services [] and, as a part of their activities, they choose to establish a business relationship with a Platform Partner. The Payees agree to the **[Terms of the Agreement]** that expressly provide that the pooled account is established in the Bank's name for the benefit of the Payees and other users. As part of this business relationship with the Platform Partner, Payees can obtain access to the pooled account at the Bank through the payment services offered by **[OpSub]**. In order for a Payee to access this account and utilize these payment services, **[OpSub]**'s **[Terms of the Agreement]** require Payees to register with **[OpSub]** and agree to **[OpSub]**'s **[Terms of the Agreement]**, either directly or through the Platform Partner, thus creating a direct contractual relationship between Payees, **[OpSub]**, and the Bank.²⁹ Accordingly, unlike the other third-party processor relationships, the Payee is not just an intermediated customer of a bank customer with no direct relationship. Furthermore, the Platform Partner, in addition to being a **[OpSub]**/**[the Bank]** customer for the reasons described above, performs referral services for **[OpSub]** and the Bank to establish these direct contractual relationships with the Payees. Thus, the Payees are provided with access to the pooled account that was established for their benefit and are customers of **[OpSub]** for purposes of applying the CIP rule. This approach is consistent with our supervisory experience and the BSA/AML risks and vulnerabilities that we have identified in the API business model that provides Payees with access to payments through a pooled account at the Bank.³⁰

²⁶ Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (Mar. 21, 2016), available at <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20160321a1.pdf>.

²⁷ See e.g., OCC Bulletin 2008-12, Risk Management Guidance – Payment Processors (2008) (describing how banks generally would be expected to monitor and perform diligence related to the processor where the bank itself lacks a direct relationship with its underlying merchants); Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual, Third-Party Payment Processors, 235 (2014).

²⁸ Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards, *supra* note 26.

²⁹ []

[]

³⁰ See *supra* note 27.

The Payors

Payor customers of the Payees are not engaged in the business of processing payments and are solely purchasing products or services offered by the Payees. The Payors do not have access to the pooled account established by **[OpSub]** under the **[Terms of the Agreement]**, are not customers of **[OpSub]**, and should not be subject to the requirements of **[OpSub]**'s CIP policies and procedures.

d. Exemption Analysis

In order to ensure that operating subsidiaries continue to operate subject to the same terms and conditions as would apply to the parent bank, the OCC will apply the exemption standard in 31 C.F.R. § 1020.220(b) to operating subsidiaries under 12 C.F.R. § 5.34. Based on the information presented by the request letter, consultation with FinCEN, and consistent with 31 C.F.R. § 1020.220(b), the OCC finds that there is a valid basis for granting the requested exemption, for the reasons described below.

First, the OCC finds that the exemption is consistent with the purposes of the BSA. **[OpSub]**'s modified CIP process of collecting partial TINs from customers does not present any additional risk of money laundering since **[OpSub]** will obtain the full TIN from a reliable third party source that will enable it to form a reasonable belief that it knows the true identify of its customer. The purpose of the BSA is "to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."³¹ The CIP rules were promulgated pursuant to Title III, Section 326 of the USA PATRIOT Act.³² The purposes of Title III of the USA PATRIOT Act are, *inter alia*:

- to increase the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism;
- to provide a clear national mandate for subjecting to special scrutiny those foreign jurisdictions, financial institutions operating outside of the United States, and classes of international transactions or types of accounts that pose particular, identifiable opportunities for criminal abuse; and
- to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities.³³

[OpSub]'s modified process will enable it to form a reasonable belief that it knows the true identify of its customer, which is a specific requirement of the CIP rule.³⁴ The only non-

³¹ 31 U.S.C. § 5311.

³² 31 U.S.C. § 5318(l).

³³ USA PATRIOT Act of 2001 § 302, 31 U.S.C. § 5311 note.

³⁴ 31 C.F.R. § 1020.220(a)(2).

compliant practice with the requirements of the CIP rules will be the incomplete collection of TINs from its customers, which is promptly addressed during the verification process by obtaining the full TINs from a third-party source. **[OpSub]** will collect three of the four pieces of identifying information required under the CIP rules – name, address, and date of birth – directly from its customers. This modified CIP process will not change the overall risk for money laundering and terrorist financing because **[OpSub]** will acquire the full TIN from a third-party source prior to establishing an account relationship and will verify the information collected as required by the rule. **[OpSub]**'s proposed practice of collecting partial TINs is similar to the existing exemption available to the processing of credit card accounts, and **[OpSub]**'s modified process should be treated similarly because the OCC finds that the rationale supporting the credit card exemption also applies to the **[OpSub]** process as described in the request letter. The credit card exemption was granted to tailor the application of the CIP rules to “situations where the account holder is not physically present at the financial institution” at account opening and involve practices that have “little risk that the lender does not know the identity of the borrower,” which is analogous to the online services provided by **[OpSub]**.³⁵

[OpSub]'s services present a low risk of money laundering given existing application of anti-money laundering regulations to the transactions that **[OpSub]** facilitates. This is because (1) the only payment methods that are supported by **[OpSub]** are debit cards, credit cards, prepaid cards, gift cards, and automated clearing house (ACH) transfers, products that can only be provided by regulated financial institutions subject to the BSA or other AML laws and (2) merchant funds are generally settled into DDAs at U.S. regulated financial institutions, which are themselves already subject to BSA requirements, including CIP rules. Furthermore, **[OpSub]** represents that it does not provide services to entities engaged in certain high-risk activities, including providing internet gambling or payment aggregation services,³⁶ which further reduces these risks. The Bank would also continue to comply with all other regulatory requirements implementing the BSA, including the requirements to understand the nature and purpose of customer relationships, to conduct ongoing monitoring to identify and report suspicious transactions, to maintain and update customer information on a risk basis, and to identify and verify the identity of the beneficial ownership of legal entity customers.³⁷

The modified CIP process does not present any additional risk for money laundering activity or terrorist financing than those present for the complete collection of the TINs. **[OpSub]** will acquire the full TIN from a third-party source during its verification process and would resolve

³⁵ The preamble to the final CIP rule notes that with regard to the credit card exception “Treasury and the Agencies have included an exception . . . for credit card accounts only, which would allow a bank broader latitude to obtain some information from the customer opening a credit card account, and the remaining information from a third party source, such as a credit reporting agency, prior to extending credit to a customer. Treasury and the Agencies recognize that these practices have produced an efficient and effective means of extending credit with little risk that the lender does not know the identity of the borrower.” 68 Fed. Reg. 25,090, 25,097 (May 9, 2003).

³⁶ The **[Terms of the Agreement]** set forth several “prohibited activities,” including providing internet gambling, payment aggregation services, and other activities that are “high risk,” that **[OpSub]** does not provide services to entities engaged in. []

³⁷ 12 C.F.R. §§ 21.11 and 163.180(d) (OCC); 31 C.F.R. § 1020.320 (FinCEN); 31 C.F.R. § 1020.210(b)(5); 31 C.F.R. § 1010.230. For example, if the Bank were to detect large volumes of unusual transfers flowing to a particular party through the **[OpSub]** service, **[OpSub]** would still be obligated to file a suspicious activity report.

any discrepancies to its satisfaction before a customer completes onboarding. Accordingly, **[OpSub]** will not offer services to an individual or entity if it is unable to obtain and verify a complete TIN. This approach is consistent with the CIP standards for credit card accounts. The OCC has also notified FinCEN of this exemption request and has considered its comments in this response.

Second, this exemption is consistent with safe and sound banking practices. The resulting banking practices will not be contrary to generally accepted standards of prudent banking operation and will not give rise to abnormal risk of loss or damage to an institution, its shareholders, or the agencies administering the insurance funds. The request letter represents that the modified CIP process will not pose additional risk to the banking system and presents limited risk of fraud because **[OpSub]**, in addition to information collected from customers, uses additional technological processes, *i.e.*, non-personal information and multi-factor verification, to ensure its customers' identity.

IV. Conclusion

In arriving at the determinations in this letter, the OCC has relied upon both its consultation with FinCEN and the accuracy and completeness of the representations made in the request letter. Nothing in this letter shall bar, stop, or otherwise prevent the OCC from taking any action affecting the Bank, including the revocation of the exemption in this letter, on the basis of information not known to the OCC as of the effective date. Furthermore, I reiterate that the Bank must continue to comply with all other regulatory requirements implementing the BSA, including the requirements to file suspicious activity reports and to identify and verify the identity of the beneficial ownership of legal entity customers.

Sincerely,

/s/

Jonathan V. Gould
Senior Deputy Comptroller and Chief Counsel