Remitly
Promises Delivered
1111 Third Avenue, Suite 2100
Seattle, WA 98101 USA

November 27, 2020

VIA ELECTRONIC SUBMISSION

Policy Division
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: FinCEN: Docket Number FINCEN-2020-0002; RIN 1506-AB41
Board: Docket Number R-1726; RIN 7100-AF97

To Whom It May Concern:

Remitly appreciates this opportunity to provide the following letter in response to the Financial Crimes Enforcement Network and the Board of Governors of the Federal Reserve System (collectively, the "***Agencies***") request for comments on the proposed rule to update the Bank Secrecy Act Funds Recordkeeping and Transfer Rule threshold requirements (the "***proposed rule***").[1]

Remitly shares FinCEN's mission to fight money laundering within financial networks, yet Remitly is concerned that the proposal to lower the Travel Rule's dollar threshold for triggering mandatory data collection requirements from $3,000 to $250 does more harm than good. We urge the Agencies to reconsider this proposal based on the reasons discussed within this comment letter. Among other things, we believe that the rule change will have a negative customer impact that harms consumer choice and and increases the costs of needed financial services, has the potential to drive remittance activity out of regulated channels to unlicensed money transmitters, and that the increased data gathering from consumers and report submission burdens exceeds the potential value for law enforcement.

Introduction to Remitly

Remitly is a licensed online remittance service provider based in Seattle. We have served over 3 million customers, many of whom are immigrants sending a portion of their earnings to support their families outside the U.S. These men and women sacrifice and save in order to provide a better life for their loved ones. When our customers send, it's not just money, it's a lifeline paying for their family's rent, a medical bill, tuition and school supplies. These services are all the more important during times of domestic and global crisis. They are a foundational part of a strong and healthy workforce in the United States and they deserve our support, particularly during the current COVID 19 pandemic. Financial inclusion is more important than ever, and Remitly is proud to offer a customer friendly product that expands access for U.S. residents to a safe and well regulated money transfer service.

1 85 Fed. Reg. 68005, October 27, 2020.

Remitly's Investment In Digital Solutions to Better Serve Customers and Fight Crime

Beyond helping to provide critical help for extended families, when remittances are sent through modern, regulated channels, such as Remitly, they strengthen our national security. Remitly, as well as other state-licensed money transmitters, invest heavily to comply with anti-money laundering ("***AML***") laws, including the Bank Secrecy Act, OFAC laws, and myriad other federal and state regulations. At Remitly, we deploy a team of highly-trained investigators, aided by the latest technology and machine learning techniques, to detect suspicious activity and report it promptly to FinCEN. Remitly is proud to support law enforcement agencies, and as a registered and regulated partner of FinCEN, with a strong risk-based AML program that is dedicated to detecting and deterring criminal activity on our platform. As a part of this effort, we work hard to share timely and relevant information necessary to fight financial crimes. So far in 2020, we have filed over 3,000 suspicious activity reports with FinCEN and we regularly partner with law enforcement to assist in investigations of potential criminal activity.

Digital money transmitters like Remitly provide an additional layer of security against consumer fraud and money laundering risk by neither accepting cash nor relying upon a network of agents to accept funds and collect customer documentation. Rather, as a digital-only provider, Remitly provides service to customers who currently possess a bank account or a debit or credit card. This approach greatly mitigates placement risk, the first stage in the money laundering process. In addition to being subject to our own Know Your Customer ("***KYC***") process that independently verifies the customer's identity with high confidence, our customers have also been previously identified and verified by a U.S. financial institution.

Remitly is a digital service provided directly to customers via a mobile application or online. As a digital remittance service, Remitly is built with consumer protection and AML, OFAC screening, and Bank Secrecy Act compliance features incorporated by design into the functionality of our product. This eliminates the vagaries and variance in compliance inherent in a distributed agent network, while also providing regulators and law enforcement with a direct and end-to-end means to verify the compliance of every transaction. Further, by accessing our service through digital means, the customer's device, location, and other digital metadata is made available to us, providing additional data points that enable us to confirm -- or call into question -- the customer's KYC information. The cumulative effect of these approaches makes our digital approach a more secure and lower risk product compared to traditional brick-and-mortar remittance services.

This risk-based approach to Anti-Money Laundering, enabled by advanced technology, is a powerful weapon to fight illegal activity. When our machine-learning models, smart rulesets, or trained staff detect something suspicious, we say something; reporting this activity to authorities as required by our BSA obligations. This reporting provides law enforcement with a high resolution view into global money flows, an invaluable tool in the fight against illegal activity, money laundering, and terrorism. Licensed money transmitters like Remitly keep the money "in the light" by efficiently processing legitimate transactions, while detecting and deterring those that are suspicious.

By contrast, it is well known that there exists an underground market of unlicensed remittances providers who do not comply with any of these obligations.[2] These informal networks operate without oversight and can be associated with black market activity. If policies are enacted that drive up the costs of legitimate remittance services or clear the field of healthy competition, money will be pushed towards shadowy alternatives.

The Proposed Rule Would Harm Consumers By Creating Barriers to Trial & Increasing Costs

While Remitly supports the aims of law enforcement and the goal of reducing illicit activity in money transmission, the proposed rule does more harm than good for several reasons. First, the proposed rule's change to mandate collection of sensitive social security or equivalent information at $250 in value transferred, from $3,000 currently, has a negative customer impact that will have the effect of chilling adoption of legitimate alternative services due to the customer trust barriers and friction creation that sensitive data collection necessarily entails. Second, the proposed rule would increase costs to consumers by virtue of the higher input costs and potential liability to regulated providers who would be required to collect and store increased amounts of sensitive customer information in an era where consumer privacy and data minimization are of increased importance.

Collection of SSN or Equivalent at $250 Will Harm Consumers by Creating Barriers to Trial

The customer impact by the proposed rule is not trivial and would chill customer trial and product adoption, particularly for newer entrants. As noted in the rulemaking, the changed threshold would greatly expand the scope of the requirement as the mean transaction size cited by FinCEN indicated a value of $588. Considering that the average Remitly transaction size is around $350, we believe that the proposed rule change would impact the majority of Remitly's customer base.

To illustrate the customer impact, consider that Remitly collects several pieces of personal information, including email, name, date of birth, and residential address during initial customer sign-up pursuant to its risk-based approach to KYC -- and thereby satisfies itself that the customer is who they say they are. A risk-based approach to KYC enables customers to access a needed financial service while also providing Remitly with sufficient information to closely monitor account activity and report suspicious activities where necessary.

Only when the customer seeks to transfer more than $3,000 -- the current travel rule threshold -- do we require customers to provide their SSN or equivalent, in addition to answering a series of EDD questions. It is our experience that at this critical stage a substantial percentage of customers will abandon the transfer request, due to mistrust associated with sharing such sensitive information with a service that is still under evaluation. It is not unreasonable to predict that a material drop in product adoption would occur at the $250 threshold if the proposed rule were to go into effect. This would harm customers who are seeking to evaluate alternative services tailored to their specific needs.

2 U.S. Department of Treasury, *A Report to the Congress in Accordance with Section 359 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.*

In addition to the literature that demonstrates why the challenge of customer trust is the critical element that the Agencies should consider when assessing the potential downsides of the proposed rule, Remitly has conducted several studies that are analogous to the increase in data collection contemplated by the proposed rule. We summarize these findings below, each of which tend to demonstrate the chicken and egg problem created by the proposed rule: if customers are required to provide this information at such an early stage of the relationship likely during the first transaction or during onboarding they may never try a product they would have otherwise considered.

On the basis of these studies, we express our concern that the proposed rule risks harm to consumer choice and financial inclusion by raising barriers to consumer trial and increasing switching costs.

Studies Show That Customers' Responses to the Collection of Sensitive Personal Data Collection Can Distort Competitive Dynamics Due to Trust

Studies have shown that if two firms offer the same value in exchange for certain data, the firm with the higher trust will find customers more willing to share that data.[3] In a 2015 Harvard Business Review article, "*Customer Data: Designing for Transparency and Trust,"* the authors found that:

> *A firm that is considered untrustworthy will find it difficult or impossible to collect certain types of data, regardless of the value offered in exchange.* ***Highly trusted firms, on the other hand, may be able to collect it simply by asking, because customers are satisfied with past benefits received*** *and confident the company will guard their data. In practical terms, this means that if two firms offer the same value in exchange for certain data, the firm with the higher trust will find customers more willing to share. For example, if Amazon and Facebook both wanted to launch a mobile wallet service, Amazon, which received good ratings in our survey, would meet with more customer acceptance than Facebook, which had low ratings. In this equation, trust could be an important competitive differentiator for Amazon.*[4]

Thus, while it is prosaic that the introduction of additional data collection fields in a product experience introduces friction into a product that reduces the rate of customer adoption, this is even more so when the data being collected is sensitive personal data such as a social security number. Consumers simply will not part with this information lightly -- and for good reason. Data breaches of even trustworthy companies have become commonplace and consumer trust in companies to protect their privacy is at a low ebb.[5]

But perhaps what is most noteworthy about the Harvard Business Review study is that past experience with a given provider is material to consumer trust. Thus, the implication of the proposed rule's data collection requirement appears likely to skew customer preferences and trial in favor of larger incumbents, a result at odds with the general policy of increasing innovation and competition in financial

---

3 *Harvard Business Review,* Customer Data: Designing for Transparency and Trust (May 2015).

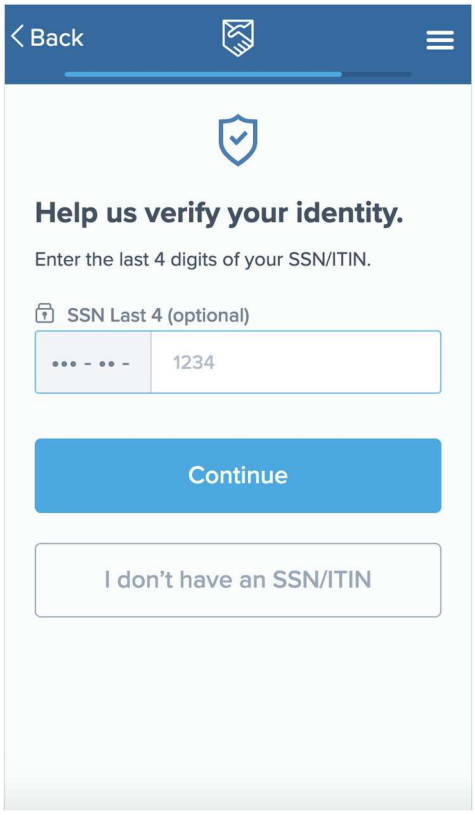
4 *Id (emphasis supplied).*

5 See *PWC*, Consumers trust your tech even less than you think (2020), available at: https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/trusted-tech.html

services. Alternatively, rather than provide this information to a regulated provider, a consumer could seek unregulated alternatives in the black market as we discuss later in this comment letter.

Remitly's "Last 4 SSN" Optional Field Qualitative Study Demonstrate Customer Concerns with Sharing of Even Minimized SSN Information

To illustrate the customer challenge described above in the specific context of international money transfers, consider the results of a study commissioned by Remitly in 2019. Remitly has traditionally collected the last 4 digits of a customer's SSN or ITIN as an *optional* field in customer onboarding. See a screenshot of the data collection screen below. This is done in order as a potential fraud mitigant and to expedite the potential for SSN verification at a later stage of the customer's lifecycle, according to Remitly's risk-based KYC approach. We studied consumer qualitative responses to that particular field. The study found customer concerns with the collection of the Last 4 digits of a customer's SSN or ITIN -- less than proposed for here.



After noticing substantial customer drop-off at this data collection field Remity commissioned an internal customer insights study to better understand the underlying concerns driving this behavior among our customer base. Specifically, we examined customer feedback from our Net Promoter Score survey, which is sent to customers immediately after their first transfer, after six months being an active customer, active six months of being dormant, or 21 days after signing up but not transacting.

The feedback from this study pointed to a trust barrier - with customer concerns around the provision of such information early in the customer relationship. Over 300 comments were collected that specifically addressed SSN and ITIN collection, each of which expressed customer trust concerns. A common negative theme among negative responses: "Don't feel comfortable sharing SSN for transfers." Even among customers who completed a transaction felt uneasy about having providing this information: "It was a fast and easy transaction, however the question about my personal ssn/itin# is something i wouldn't provide and made me feel a bit uneasy" and "It's fast but i didn't like that you requested my ssn." These common concerns demonstrate the importance of consumer trust in soliciting sensitive customer information and the challenge of establishing it in a new relationship.

Following this analysis, Remitly commissioned a customer feedback panel of six participants. In this portion of the study, participants were presented with the Remitly product from initial landing page through to transfer submission. Participants were asked to share their thoughts as they progressed through the transfer flow, as well as whether they would stop using the app on any page if they were

actually using it in real life. They were then returned to the optional "Last 4 SSN/ITIN" collection step described above and asked why people might have concerns about sharing this information.

Half of panel respondents expressed concerns regarding the "Last 4 SSN" data collection step. Concerns raised included the risk of identity theft, that this information will be used for "unknown" purposes, and discomfort that the company will then have their SSN/ITIN information in addition to their personal, mailing, and payment information. Slightly offsetting the concern, one third of participants noted that they felt more comfortable in sharing this information because it was "only" the last 4 digits of SSN that were requested. Finally, among all participants, this was the only point in the Remitly product at which respondents said they would stop using the service, which is notable in that other identifying information and payment information are required data elements. This tends to demonstrate that there is something uniquely sensitive about a customers' provision of SSN, even to the point that a partial SSN collected optionally caused consumers with concerns regarding adoption of the service.

In sum, this study tends to demonstrate that consumers have significant concerns with sharing even a ***portion*** of their SSN with a remittance provider, even if the provision of that information was entirely optional.

Remitly's "Last 4 SSN" Optional Field Product Experiment Showed That Some Customers Will Not Complete Onboard If This Information is Requested At That Stage

Drawing upon the lessons learned in the consumer insights study discussed above, Remitly ran an "in product" experiment to determine whether these qualitative findings would extend to how consumers actually respond to the request for such information in a live transaction environment.

The hypothesis for this experiment was that, given the above qualitative feedback, if Remitly were not to request the Last 4 of customer SSN or ITIN from customers, that it would increase the number of customers who onboard and the rate at which customers complete orders. The control and treatment approaches associated with this are provided below, with one set of consumers receiving the 'standard' experience which includes the "Last 4 SSN/ITIN" collection step and the treatment group not being asked to complete that step.

This product experiment was run over several weeks, allocated across a split of new customer onboarding experiences across Remitly's web and mobile app platforms. After customers had been allocated across the control versus the treatment experience, we summarized the results. We found that the removal of this optional data collection step had the effect of *increasing* overall order completion rate with a high degree of confidence. That is, more customers would complete transactions if not prompted for this information, even when this information was requested purely on an optional basis. If extrapolated across Remitly's U.S. customer base, it was estimated that this change would result in thousands of additional customers using Remitly that would not otherwise have completed onboarding. We would be willing to provide additional information regarding this experiment upon request.

This experiment demonstrates that even minor, optional changes in information collection related to SSN elements can have material impacts upon product adoption. If one were to extrapolate these results

across the industry, it is apparent that the proposed rule would have substantial competitive impacts. Given the above qualitative and quantitative data associated with the optional data collection of merely the "Last 4 of SSN", it would be expected that the noted effects would be greatly exacerbated.

Enhanced Collection of Personal Data Poses Customer Privacy and Cost Concerns

The change in threshold for recordkeeping of sensitive information from $3,000 to $250 for transfers would substantially increase the universe of consumers that MSBs like Remitly held their most sensitive information. For example, Remitly's average transaction size is $350, meaning that nearly all customers would have their SSN or equivalent transmitted and stored in order to meet the proposed rule's requirements. This increases the potential damage that could occur to consumer privacy and MSBs in the event of a data breach, as more customer data will be on file with more providers.

An IBM study estimated the cost of a data breach to a provider at $150 *per customer record*,[6] which illustrates the potential downside liability that accompanies the significant expansion of collection and retention of sensitive personal information. While we and others in our industry invest significantly to appropriately secure the sensitive customer data we are required to keep on file, the reality is that such protections are not infallible. It should also be apparent that the means to securely store such data do have costs that would be passed through to consumers in the form of higher prices.

The cost to insure money transmission businesses such as ours will increase as the number of sensitive records will increase substantially as cybersecurity policies are also generally priced with regard to the number of sensitive records kept.

The Proposed Rule Will Weaken Transparency

The proposed rule would lower the funds threshold for recordkeeping from $3,000 to $250 for transfers beginning or ending overseas. While difficult to quantify, there is a legitimate concern that the proposed rule will raise customer switching costs and product costs, which may incent a movement of customers toward less transparent systems, potentially harming the agencies' financial crime-fighting reach.

As the Treasury Department found in its study of the Informal Value Transfer Systems ("***IVTS***"), which operates as an alternative "black market" to the regulated money transfer system:

> *U.S. citizens and persons residing in this country from nations in which the use of IVTS is commonplace use the system for various reasons. In countries lacking a stable financial sector or containing substantial areas not served by formal financial institutions, IVTS may be the only method for conducting financial transactions. For example, foreign aid money going to Afghanistan is being disbursed through IVTS due to a lack of a banking infrastructure.* ***Individuals and organizations often use IVTS*** *due to the existence of inadequate payments systems, to avoid foreign exchange or capital controls, and* ***when the formal financial sector is not readily accessible, significantly more expensive, or***

6 IBM Security, Cost of a Data Breach Report (2020), available at: https://www.ibm.com/security/digital_assets/cost_data_breach-report/#/

more difficult to navigate.[7]

By increasing the data collection requirements for legitimate, regulated providers, there arises a perverse incentive among consumers who are distrustful of providing such information to rely instead upon the alternative informal market of providers where this information is not collected.

We submit that the combination of a risk-based KYC approach, supplemented by the existing Travel Rule threshold of $3,000 strikes the right balance between collecting sufficient information to meet law enforcement objectives. A risk-based system provides flexibility that can be adjusted on a case by case basis accounting for the risk of the customer, during and after initial sign-up.

A risk-based approach enables industry and government stakeholders to have visibility into funds flows and creates an opportunity for stepped-up recordkeeping when suspicious activity is identified or when a customer seeks to send amounts greater than $3,000. These approaches maximize the agencies' reach by bringing as many customers into a regulated environment, rather than potentially diverting traffic to less transparent and unregulated systems.

The Facts Do Not Demonstrate a Concrete Benefit for the Modified Data Collection Thresholds

While the potential costs to consumers of the proposed rule appear to be substantial in terms of barriers to trial, consumer privacy, and increased costs, the purported benefits of the proposed rule appear minimal on the record presented.

The Agencies argue that some suspicious activity has been associated with transfers below the $3,000 threshold. However, the data do not demonstrate that having the additional information associated with such transactions would be helpful to fighting crime in any specific way; rather, it suggests only that such information *could* be helpful, without any analysis of government or industry capabilities to identify suspicious activity and act upon it.

The cases cited in the ANPR do not provide evidence that the collection of this information would be useful. Rather, the cases cited are examples of the *successful* identification of individuals sufficient to obtain an indictment in spite of the absence of the very information now deemed necessary to be collected. By contrast, Remitly respectfully submits that cases cited tend to demonstrate that a risk-based approach to KYC enables MSBs to file SARs with law enforcement containing sufficient to positively identify, locate, and prosecute the offending individuals. If anything, the cases cited tend to demonstrate that the current risk-based system to identification is working as intended in terms of providing timely and useful identifying information to law enforcement.

The Agencies note in the proposal that some providers in the space -- presumably referring to banks who are required to collect this information under Agency CIP requirements -- already collect SSN information at account opening.[8] However, this argument does not accord appropriate weight to the fact that such

7 U.S. Department of Treasury, *A Report to the Congress in Accordance with Section 359 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, at pg. 5 (emphasis supplied).

8 FFIEC, *BSA/AML Examination Manual, Customer Identification Program.*

an approach to information collection is explicitly *not* mandatory for MSBs pursuant to their own risk based BSA/AML compliance programs. Indeed, the CIP Rule explicitly states that accounts requiring such data collection do not include "a product or service in which a formal banking relationship is not established with a person such as a… wire transfer[.]"[9] Indeed, there are good reasons, described above, as to why an MSB might wish to defer the collection of sensitive information until such time as a more substantial relationship has been established.

Finally, the data presented in the proceeding do not offer any evidence that additional recordkeeping will further law enforcement objectives. A focus on quality analysis of existing information would be a better use of industry and government resources with lower total costs to all, rather than arbitrarily requiring more quantity of information collection on all customers that could theoretically be useful at some point.

By contrast, we note that the submission of high quality SARs is not dependent upon the inclusion of SSN. As noted previously, we have submitted over 3,000 SARs to FinCEN in 2020, the majority of which contain sufficient verified identity elements name, address, date of birth as well as as other transactional data, identifying metadata, and accompanied by a narrative prepared by expert investigators, all collected pursuant to a risk based KYC program that enables law enforcement to identify, locate, and prosecute the offending individuals. We respectfully suggest that FinCEN should take comfort that the risk based KYC programs required of MSBs across our industry is working as intended and provides the level of identifying information necessary to successfully execute its law enforcement mandate.

Financial Inclusion and Illicit Funds Oversight Should Be Mutually Beneficial

Remitly notes that the proposed rule does not consider the rule's impact on financial inclusion. Given our findings that customer choice is likely to be harmed by the increased data collection requirement, Remitly believes that the impact upon financial inclusion merits the Agencies' consideration.

Remitly believes that risk-based approaches that allow companies to serve customers in need while targeting enhanced oversight when risks are identified results in a more inclusive financial services marketplace as individual providers seek to offer products that are tailored to their unique customer bases. Rather than impose a prescriptive requirement, the agencies should instead seek to provide industry with the flexibility to establish customer relationships and then adjust oversight mechanisms pursuant to the risk-based approaches appropriate to products and customer bases as set forth in their BSA/AML programs.

This approach enables providers to tailor approaches to low risk transactions and bring more of those transactions into the regulated financial system, while simultaneously maintaining the flexibility of a risk-based approach that is the hallmark of our anti-money laundering regulations.

***

9 *See* 31 CFR 103.121(a)(1)(ii).

Remitly appreciates FinCEN and the Agencies' work to improve recordkeeping requirements and looks forward to working with the agencies to meet its crime fighting mission while also weighing the interests of consumers and promoting greater financial inclusion. Thank you for considering our views.

Respectfully Submitted,

Aaron M. Gregory
General Counsel