Wise US, Inc.
19 West 24th Street, 9th Floor
New York, NY 10011
www.wise.com
rina.wulfing@wise.com

June 30, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, DC 20219

James P. Sheesley
Assistant Executive Secretary
Attn: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

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

Comment Intake
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Response to Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning

OCC: Docket ID OCC-2020-0049; Federal Reserve System: Docket No. OP-1743; FDIC: RIN 3064-ZA24; CFPB: Docket No. CFPB-2021-0004; NCUA: Docket No. NCUA -2021-0023

Wise US, Inc. (Wise) appreciates the opportunity to submit comments to the Board of Governors of the Federal Reserve System (Federal Reserve), Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) in response to the request for information and comment on financial institutions' use of artificial intelligence.

We applaud the financial regulatory agencies for facilitating a conversation on use of artificial intelligence (AI), including machine learning (ML), in the financial sector. Wise uses these

tools to fight fraud and money laundering, and has weighed in with financial regulators in the past regarding how policymakers should embrace AI and ML to fight financial crime through modernized guidelines and increased information sharing. AI/ML allows us to more comprehensively consider risk factors and our customers' transactions, leading to faster identification of risky behavior while lessening impact on good customers. We have concerns, however, that outdated regulations and explainability requirements continue to negatively impact our model's effectiveness and our ability to quickly adapt to new risks.

Background

Wise is a global technology company, building the best way to move money around the world. With the Wise account, people and businesses can hold 54 currencies, move money between countries and spend money abroad. Huge companies and banks use Wise technology too; an entirely new cross-border payments network that will one day power money without borders for everyone, everywhere. However you use the platform, Wise is on a mission to make your life easier and save you money.

Co-founded by Taavet Hinrikus and Kristo Käärmann, Wise launched in 2011 under its original name TransferWise. It is one of the world's fastest growing tech companies having raised over $1 billion in primary and secondary transactions from world leading investors.

Wise US, Inc., our U.S. entity, is a licensed money transmitter in 48 states[1] and otherwise authorized to provide such services to customers in the remaining states and territories. 10 million people and businesses use Wise, which processes $7 billion in cross-border transactions every month, saving customers over $1 billion a year. Wise has over 2400 employees in 14 offices, including sizable offices in New York City and Tampa, Florida.

Comments

Wise incorporates AI, in particular ML, in assessing financial crime. We appreciate the opportunity to respond to regulator questions as an international payments processor continuously evolving to keep our products safe. ML helps us prevent, detect and deter financial crime, allowing us to more comprehensively consider the risk factors of our customers and their transactions. This leads to better identification of risky behaviour.

How Wise Uses ML

Currently, our fraud and anti-money laundering (AML) control functions use ML. Our ML system uses over 110 data points, with each data point assigned a risk aspect. When a customer displays certain behavior, our system flags this as suspicious and creates cases for

[1] Wise US. Inc. only offers its services in the states in which it is licensed or in the states that do not currently require it to be licensed. which includes all states except for Nevada. where a partner financial institution offers a Wise-branded money transmission service. and Wise Ltd.. Wise's UK parent. which is regulated by the FCA. acts as a service provider to that financial institution.

our internal investigations team. Our investigations team reviews the case, and if financial crime is found to be occurring, the customer is quickly offboarded and we file a Suspicious Activity Report (SAR). Our series of ML rules have scaled along with Wise's own growth, which has resulted in more advanced customers and businesses with more complex typologies. This also means we are a target of more advanced financial crime, necessitating a more advanced and quickly evolving system.

Oversight is of utmost importance to our ML controls. Compliance is one of our largest teams at Wise and we have not been subject to an enforcement action to date. All staff receive training on how to identify possible criminal activities, and a clear escalation process is in place internally for any issues. We conduct intensive model validation exercises with an advanced Model Validation Team, who are trained in identifying the evolution of our ML rules and drilling down into specific cases. We have a named Money Laundering Reporting Officer responsible for liaising with relevant authorities where we have suspicions of criminal activities. To keep improving our systems and controls, we regularly commission audits from specialised external consultancies and audits. Our ML controls are set at a global level, which enables us to take a consistent approach across different countries.

To ensure our rules are explainable to regulators and third parties and to avoid any possible gaps in our controls, we operate a hybrid system, where our ML rules operate alongside more traditional static rules. Our ML rules are almost twice as precise as static models, speaking to the power a ML system could have.

In a static system reflective of U.S. law and current recommendations, monitoring rules address a particular money laundering typology. Take for example a hypothetical flag of when a customer is in Brazil and transacts over $100,000 in three days. This creates a static decision tree output, which in this case would look like:

> *Create AML_suspicion flag if: country == Brazil AND 28_day_transaction_volume > 10000 AND total_recipients_count > 3 AND business_type == (construction OR unknown)*

In this decision tree example, a binary static rule would not flag a customer only transacting $99,000, or if a transaction of $150,000 across 33 days. In contrast, a ML system has a learning curve, where the system learns from current cases with input from our team. Because it quickly learns to focus on bad customers who have other attributes that create reasonable cause for suspicion, the ML system would flag cases like this, despite the example being outside of the binary rule.

As an innovator by nature, Wise uses modern technology to fight financial crime, creating an effective system that uses ML to evolve and stay in lockstep with financial criminals. We use ML to catch constantly evolving threats, but unfortunately, there are several significant problems we frequently encounter with current regulations. Specifically, we face issues with

static rules, a lack of information sharing, and a lack of clear guidelines and definitions for using AI/ML for transaction monitoring.

Explainability - Evolving Away From Static Rules

As mentioned above, a static system reflective of U.S. law and current recommendations is not prepared to catch advanced financial criminals. For financial services companies strictly following U.S. monitoring rules, this means companies are fighting the last war on many typologies, since financial crime prevention is by nature a dynamic game.

Static monitoring rules based on the regulatory system are not self-learning and not able to generalise, nor do they keep up with ever-evolving financial criminal models. Static rules create the illusion that financial institutions have covered all potential risks when in reality, advanced bad actors have evolved past our current system. Good customers are more likely to be flagged while more sophisticated bad actors can evade detection by identifying the patterns and risk factors that static rules are looking for.

Financial companies have the critical responsibility to prove to regulators they are covering certain types of typologies. Unfortunately, in order for regulators to understand the safety of our products, static rules are often necessary, as the regulator has an easier time identifying them. This cannot be the standard - while the desired feature of these rules is clear explainability, a ML system learns and evolves constantly as a default. It is much better at recognizing difficult and well hidden financial crime, but larger and more complex datasets that make up advanced ML systems make explainability more challenging. This forces companies to weigh a trade-off between explainability and performance, resulting in a disservice to customers who are better protected by the use of ML. Regulators must be prepared to take into account dynamic updating techniques.

Due to issues with explainability, Wise's use of AI/ML is generally "in addition" to existing controls that are known and more easily tested by regulators. This may have the inadvertent effect of hindering the adoption of technology that could better fight financial crime. We are negatively impacted in our abilities to evolve our system by the requirement to explain the system to regulators who aren't up to date with financial criminals and their use of technology.

There must be a co-evolution of understanding ML and using it for financial crime, and the ability to explain the safety and soundness of the system to regulators. Regulators should consider how to expand the parameters in which payment services providers can explore ML with the goal of eventually replacing static rules. Any replacement rules must have a more robust methodology and be dynamic from the start. We cannot afford to fall behind financial criminals.

Improving the Suspicious Activity Reporting (SAR) Regime

Increased information sharing between law enforcement and financial institutions has long been a topic of discussion within the fraud/AML community. For example, in the United Kingdom, there is a detailed plan being coordinated by government and private industry to create a SAR framework and database[2] from which to draw intelligence. If law enforcement such as FinCEN could provide databases of information for ML to learn from, that could be ground-breaking to improve controls to detect and fight crime. FinCEN and law enforcement do have information sharing portals, but the updates are occasional and with the primary purpose of facilitating information sharing between banks. More substantive updates from law enforcement with a greater level of detail would help financial institutions better combat financial crime and improve the federal regulators' oversight of Bank Secrecy Act (BSA) and AML compliance.

Increased information sharing between financial institutions could also help these institutions build more efficient and accurate AI and ML algorithms. The lack of transparency and data sharing makes it hard to predict patterns across multiple financial institutions, which in turn makes money laundering and fraud prevention more difficult. Wise uses automated data detection methods to analyze repeat patterns or behaviors, and our ML models are constantly being trained to identify and detect suspicious patterns of activity using over 110 data points for consideration. We use this data to proactively engage with relevant external parties including our financial partners and law enforcement, for example sharing with law enforcement our learnings and typologies of financial crime. We believe an accessible, regularly updated, and substantive database provided by law enforcement that also includes a framework for financial institutions to share their data would vastly improve controls to detect and fight crime.

Creating a Third Party Framework

We partner with banks who, while they trust our controls, also feel the need to do their own screening for transactions initiated on their platform out of an abundance of regulatory caution. We also utilize the services of third parties and their technology to verify customers. Many of our legacy banking partners don't have as much experience with ML, and we are consistently slowed down by needing to explain specific approaches to ML on our platforms. Due to static rules, our technology and monitoring continuously must evolve past what has been defined by law and as a result remains high performing, but because there isn't a clear standard set out we often raise questions with our partners and regulators about whether we have standard screening practices.

As more financial technology companies partner with banks, or institutions offer services through each other's platforms, building a solid third party reliance framework on verification

[2] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version

is in line with recommendation 17[3] from the Financial Action Task Force (FATF). This allows regulated institutions - both at the state and federal level - to work together to better mitigate and prevent financial crime without having to verify customers multiple times or recreate systems.

Developing Clear Regulatory Definitions

Additionally, the regulatory framework and Federal Financial Institutions Examination Council (FFIEC) examination manual should be updated to reflect the value of modern technology. At a minimum, ML and AI should be more clearly defined, and there should be more explicit references to modern identification tools that help combat financial crime. For example, selfie with identification is an increasingly common and effective form of identity authentication. Since the current rules lack references to modern tools, we go to great lengths explaining and demonstrating the technology and its effectiveness to our bank partners. This means that while our controls are more time effective and may actually be stronger, through our use of technology, our bank partners are more comfortable with a manual document review process because it's how they've long operated. Without clear guidance and a regulatory reference, banks will be slow to change their approach to managing risk, which keeps our financial system vulnerable to financial crime. Giving AI and ML regulatory definitions will help us explain their use, and also mean consumers are better protected against poor governance around automated decision making and bias.

* * *

We appreciate the opportunity to provide our comments on the efforts of the federal financial regulators to consider modernizing rules on AI and ML. Please do not hesitate to contact us if you have any questions regarding these comments or if we can be of any assistance.

Best,
Rina Wulfing, Policy and Campaigns (North America), Wise
Danielle Herndon, Global FinCrime Product Compliance Lead, Wise

[3] https://cfatf-gafic.org/index.php/documents/fatf-40r/383-fatf-recommendation-17-reliance-on-third-parties