November 7, 2019

Via Electronic Submission

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

RE: Docket No. OP – 1670 Potential Federal Reserve Actions to Support Interbank Settlement of Faster Payments, Request for Comments

Dear Ms. Misback,

SAS Institute[1] (SAS) welcomes the opportunity to submit this comment letter to the Board of Governors of the Federal Reserve System (Fed) in response to the Request for Comment (RFC) regarding the potential Federal Reserve actions to support interbank settlement of faster payments. Millions of individuals and small businesses across the US will stand to benefit from this *significant* announcement. Building a new, round-the-clock payment and settlement service for financial institutions to access reinforces the importance of these financial institutions today and in the future. Moreover, the complex nature and sophisticated fraud schemes are mounting and better protecting checks, automated clearinghouse (ACH), and funds transfer services from banks and non-banks will ensure our financial system is secure going forward.

Given our long-standing relationship and experience working with the Fed, the Federal Reserve Bank system, and many financial firms globally, we are both optimistic and aware of the challenges that building a real-time payment and expansion system will bring. As we shared in our last RFC in December 2018, we believe SAS' strengths in fraud-monitoring and risk management expertise will enhance the Fed's multi-year move to a 24/7/365 real-time environment by providing a "ubiquitous, safe, fast and efficient" framework. While there are a number of important considerations for this new environment and implications for the global financial system, we are limiting our commentary to outline the best practices for enhancing and detecting fraud risk in a real-time payments environment.

The approximately 10,000 financial institutions in the U.S. are under tremendous threats today that will only increase in sophistication and severity in the future. Therefore, developing this new interbank 24/7/365 real-time gross settlement (RTGS) with integrated clearing functionality, called FedNow Service, requires monitoring and mitigating the threats of the future. Strong security measures will have to detect the rise of real-time fraud given the introduction of increased transactions. Furthermore,

[1] Headquartered in Cary, North Carolina, SAS is the largest privately held software company in the world. Committed to providing cutting edge analytics solutions to its customers, SAS invests an unparalleled 26% of revenue back into R&D. Our mission is to deliver superior software and services that give people the power to make the right decisions. For over 40 years, SAS has established itself as one of the leaders in advanced analytics and data management, a standard that has been repeatedly recognized by independent third-party researchers, including Gartner, Forrester and Chartis Research.

SAS Campus Drive
Cary, NC 27513 USA
www.sas.com

financial institutions are not perfect and do facilitate improper payments that must be appropriately managed by all parties.

The Federal Reserve should consider an enterprise balanced fraud model based on several key approaches:

- **Prevention**: Ensure there are appropriate risk policies, controls and capabilities to make fraud risk tolerance as low as possible to promote trust in the new payments service.
- **Detection**: Use the payments information and SAS' analytics to accurately identify high risk transactions, accounts, networks and contact the appropriate entity for treatment in real-time. Leverage machine learning techniques to improve create / suggest intelligent / adaptive rules.
- **Advocate**: Create a quick resolution process to mediate disputes between banks.
- **Recovery**: Have a timely process across the banks to mitigate and recover funds on behalf of customers/clients or the bank.
- **Controls**: Have the necessary monitoring tools for 24/7 operations management and cross-bank communications. Have a Security and Protection Framework process to identify risks and close gaps. Create a fraud risk monitoring process to quickly identity emerging threats and collaborate with appropriate entities to resolve. Provide Industry benchmarking on key transaction and fraud metrics.

We believe the Federal Reserve is seeking a business and technology partner to help implement an enterprise solution for assessing enterprise fraud risk on its Real-time Payments system that leverages all monetary and non-monetary transactions placed through the system. The solution must have the flexibility and expandability to support and leverage this transactional data. It must also have the capability to create and run sophisticated modeling techniques to develop scoring and alerts which will then notify participant Financial Institutions (FIs).

Fraud and financial crimes are a top three investment priority at SAS. Our approach is unconventional in the software industry as SAS is the only financial crimes software vendor with the resources and private sector expertise and discipline to build out the necessary components to mitigate the future regulatory and fraud challenges facing the banking industry. Some of the fraud risks that will be evident in this new real-time environment are some of the same risks we see today. Building data driven tools across banking, retail and manufacturing provides SAS with a comprehensive understanding of the danger businesses must deal with. Our proven track record in successfully working with government at the federal and state level gives us insight into how policymakers and regulators must confront schemers to protect individuals. Though a real-time payments system environment will have clear benefits, they also create new opportunities for fraudsters to steal funds and digital identities. Common financial crimes FedNow will need to monitor are:

- Account Takeover (ATO) schemes
- Synthetic identities
- Social engineering
- Money Mules

Account Takeover (ATO) schemes

Bad actors will gain key authentication credentials (username, passwords), then use Account Takeover (ATO) schemes to gain access to accounts and exfiltrate funds by taking advantage

of real-time payments rails. ATO fraud is very popular today due to the rise of digital commerce and online payments. This allows fraudsters to cloak the sources of their funds from authorities as they quickly move them between different accounts.

What looks risky?

- A customer's email or telephone number that is connected to their account recently changed.
  - Online access at off hours. These are actions that would be unusual for the legitimate user.
- A customer stops getting calls, texts and emails.
  - Fraudsters conduct a SIM swap or forward calls at the Mobile Network Operators.

Controls to Deploy

- Banks must implement multi-factor authentication (including behavior analytics), create robust security protocols, and have endpoint device detection.
- Banks must have strong authentication, leverage device fingerprint and malware detection tools.
  - Leverage One Time Passcodes (OTP) to improve authentication.
  - Leverage 3rd party vendors for digital identity and email addresses.
- Deploy network analytics at the Federal Reserve to monitor both sides of the transaction.
- Leverage data analytics to establish patterns of normal and risky behavior.
  - Data visualization, exploration, segmentation.
  - Link analysis for entities and networks.

- Will FedNow monitor for and leverage cross-bank 'negative' files in real-time?

Synthetic identities

The fraudster combines both real and fictitious data to create an identity. They will then "cultivate" the identity to make it appear authentic and mature what appears to be a good credit profile.

What looks risky?

- Multiple accounts opened using the same SSN, Device, IP Address.
  - SSN, Address, Phone mismatches.
- Identity has a 'thin credit file' and social media presence is not deep.
- Online applications completed more quickly than usual (Bot detection).
- First payment default or bust-out fraud found in the Collections Dept.

Controls to deploy

- Require banks to have a better KYC process / 360-degree view of their customers.
  - Know their behavior. Leverage digital and behavioral information to understand the preferred path(s) that customers utilize.
  - Leverage information to identify when a new 'authorized user' has been added.
  - Monitor for accounts with similar SSNs, Addresses, Phone Numbers.
- Leverage industry 'negative files' of known bad identities.
  - Will FedNow allow a portion of highly risky transactions to be delayed for a short period of time if there are multiple red flags?

Social Engineering Leading to Account Access

Social engineering, in the context of information, is the manipulation of people into performing actions or divulging confidential, usually personal information.

What looks risky?

- *Phishing* - a malicious attempt to access a person's personal and sensitive information such as financial credentials. The attacker behind a phishing attack poses as an authentic identity or source to fool an individual. This social engineering technique involves email spoofing or instant messaging to the victim.
- *"Tech Support"* - involves fraudulent attempts to scare people while putting them into the thought that there is something wrong with their device. Attackers behind this scam try to gain money by tricking an individual into paying for the issue which doesn't actually exist.
- *Clickbait* - in this method, the attacker sends an enticing ad related to games, movies, etc. Clickbait is most seen during peer-to-peer networking systems with enticing ads. If you click on a certain Clickbait, an executable command or a suspicious virus can be installed on your system leading it to be hacked.

Controls to Deploy

Customers should have updated anti-virus software as well as enabled Spam filters.

Leverage big data analytics to establish patterns of normal and risky behavior. Watch for sender account destination of country, amount, same day of the month payments, established vs immature relationship with beneficiaries. For the online 'user' (the fraudster), monitor device fingerprint, browser data, payment template details and mismatched authentication signals.

Money Mules

"Money mules" are used to transport and launder stolen money. Criminals recruit money mules to use stolen information to extract funds through branch, ATM, or online means. Individuals being used as money mules may be 1) unwitting/unknowing; 2) witting; or 3) complicit.

What looks risky?

Most solicitations are disguised as "work from home" opportunities as well as other scams (e.g. online dating, lottery, reshipping, Business Email Compromise). These advertisements often target unsuspecting people who are interested in the convenience and flexibility of these types of jobs. Because there are companies that legitimately offer opportunities to work from home, users may not recognize malicious offers.

Controls to Deploy

- Leverage data analytics to establish patterns of normal and risky behavior (use digital and biometrics).
- Leverage industry 'negative files' of known bad identities.
- Originating bank will need to look for wires into the mule account followed by funds being split into numerous transactions which could include additional wires, cash, or virtual currencies.

The Fraud Management Solution

As discussed, the complex and sophisticated nature of financial crimes is mounting. SAS Fraud Management solutions could provide the Federal Reserve with the capabilities to deploy fraud risk decisioning rules and models with a *real-time* engine.

SAS Fraud Management is a full-service, enterprise solution, with the capabilities to monitor multiple products/transactions on a single platform and is the only fraud solution available that offers 100% real-time scoring and decision capabilities. SAS achieves 100% real-time scoring by engineering the in-memory solution to meet capacity and volume needs.

The Federal Reserve's fraud management solution should operationalize analytics (models created by the Federal Reserve or by SAS) to render score-based "intelligent" fraud decisions. The Federal Reserve can harness the power of the SAS Scoring Engine to feed scores, actions, reason codes, and other data elements to other decisioning platforms.

Enhanced Decisions Through Data Orchestration: Our solution includes a real-time data orchestration utility – SAS Business Orchestration Services (BOSS) – that will simplify the Federal Reserve's ability to bring in *any* type of internal data and/or third-party (including large quantities of structured and unstructured data) to help the Federal Reserve use data as an asset in both fraud decision rules *and* analytics.

SAS already provides services to The Federal Reserve on a Do Not Pay file that could be integrated into the FedNow service as another risk control in real time. These files should be queried if The Federal Reserve stands up a real time payment environment.

SAS works side by side in partnership with customers to help with decisions on how to best leverage solutions within their existing architecture and application infrastructure. The solution includes:

- Highly functional fraud alert management and investigation system
- Extensive reporting capabilities
- New, flexible connectors to plug into current production systems

Solution Overview: A fraud management solution should be architected to support an enterprise-wide deployment of fraud monitoring and controls through:

- Message Layout/Application Program Interface (API) to capture multiple types of transaction types, regardless of product or channel.
- Metadata-driven architecture which ensures data consistency, usability, repeatability, as well as the capture and reuse of relevant customer data.

The Federal Reserve should consider a solution designed as an end-to-end solution offering decision rules, analytics, decisioning, alert management, and integration to other systems in a single enterprise platform. Numerous components collectively comprise a SAS solution. At the core is a multi-tier architecture design. All components are designed to be tightly integrated but loosely coupled to leverage best-of-class availability and reliability, scalability, and maintainability goals.

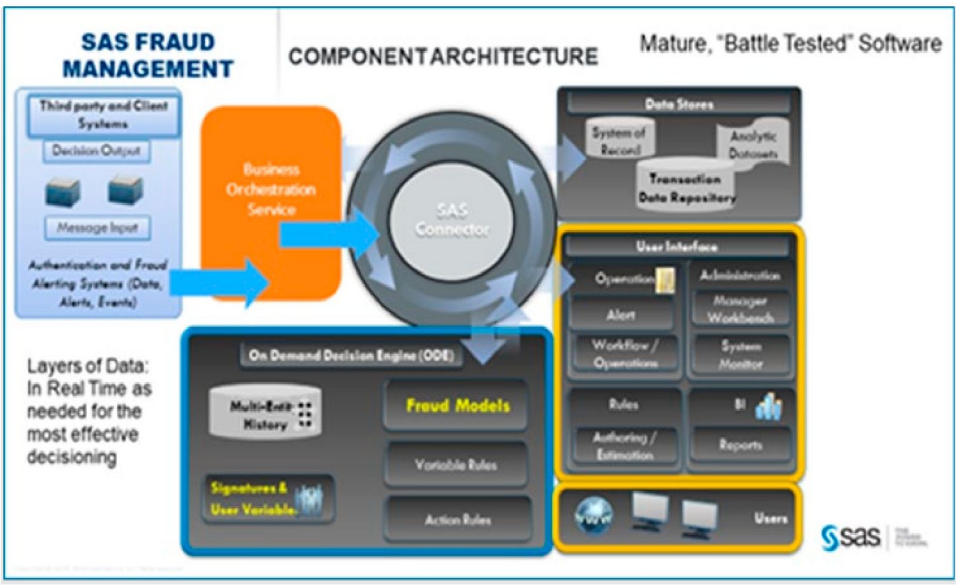

Figure 1 - The SAS fraud solutions is made up of several components.

The Federal Reserve's solution should feature many tightly integrated but loosely coupled complementary components:

- Open systems (Java-based) or Mainframe (COBOL-based) SAS Connector.
- OnDemand Decision Engine (ODE): SAS OnDemand Decision engine, coupled to the SAS Connector, controls the execution of analytic models and real-time user-written and system rules.
- SAS Analytics: Innovative, patented modeling technologies and approaches to meet customers' requirements and to ensure they benefit from the very best levels of fraud detection performance.

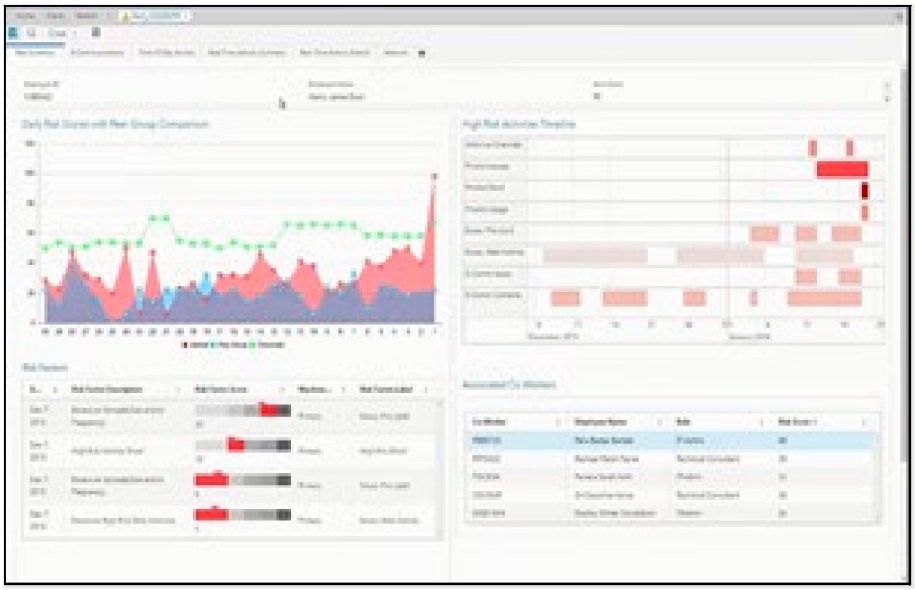

Figure 2 - Rules Studio Interface

- Rules Studio: User interface for permitted users to write rules and simulate effects using production and historical transaction data. User-defined rules in the solution can be developed, tested, analyzed, amended, made 'production ready,' and cancelled using the Rules Studio user interface (UI), independent of all IT or other third-party resource requirements.
- Alert Management (Analyst Workstation and Manager's Workbench).
- Multi-Entity History (MEH): A relational database which stores the historical analytic attributes at multiple entities (e.g., customer, account, payer/payee, beneficiary, device, etc.) for a holistic 360-degree view. Used during analytic model and business rules execution in all processing modes (e.g., real-time, near real-time).
- Transaction Data Repository (TDR): A relational database that together with the SOR database comprises the operational data store suite of the SAS solution. The TDR stores all transactions that are processed by SAS Fraud Management and is used for presentation in the browser-based user interface during alert triaging.

In conclusion, we applaud the Federal Reserve's vision to develop and promote a ubiquitous, safe, fast, and efficient real-time payment system in the US. Financial crimes and complex schemes will present an ever-growing set of challenges for individuals, governments and businesses. Introducing real-time payments will, unfortunately, open the door to fraudsters who seek to abuse countless victims. The required tools to detect and curb these schemes must also be done in a fast and efficient method. No one can predict the future of financial services, but many people and businesses will rely on FedNow so it's important to protect them. In addition, the Federal Reserve acknowledges that the payment systems used today, primarily check, ACH, wire, and credit cards might not be the payments of the future. Building a real-time payment environment must consider not only the technology and threats of today but also payment rails of tomorrow.

Again, we appreciate this opportunity to submit comments to the Federal Reserve on potential actions we recommend to facilitate real-time interbank settlement of faster payments. We welcome the opportunity to further discuss how SAS can support the Federal Reserve on this effort, please feel free to email or call the undersigned with any questions regarding these comments.

Sincerely,

Thomas French
Industry Consultant, Fraud and Financial Crimes
thomas.french@sas.com
(980) 938-1811

Austin Tuell
Sr. Account Executive, Financial Technology
austin.tuell@sas.com
(212) 413-2571