FIS Bill Pay Fraud Monitoring Service

June 2017

www.fisglobal.com

Table of Contents

FIS BILL PAY FRAUD MONITORING SERVICE **1**

OVERVIEW **3**

Monitoring Services 3

Transaction Suspension *4*

Client Responsibilities *4*

Additional Tools *5*

Implementation Requirements 5

Real-Time Scoring *6*

Reporting 6

MTD Fraud Alert Volume (FRD-001) *6*

MTD Fraud Alert Volume (FRD-004) *6*

Fraud Report (FRD-002) *6*

Suspected Fraudulent Transactions Report (SFRD-001) *7*

© 2017 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide. This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction or distribution to third parties is strictly prohibited.

OVERVIEW

As financial institutions offer new and compelling products to consumers with the goal of increased speed and access to monetary transactions, mitigating the risk associated with these products is imperative. To that end, within Payment Manager, FIS™ offers one of the premier fraud monitoring services available in the market today. The FIS Bill Payment Fraud Monitoring Service includes transaction monitoring and alerting for fraudulent activities associated with all scheduled bill payment transactions including:

- New account consumer scam fraud
- New account identity theft fraud
- Unauthorized access
- Account take over

The FIS Digital Payments Fraud Monitoring team has years of industry knowledge and expertise, uniquely qualifying them to detect and prevent fraud within FIS's Payment Manager. The FIS fraud analysts use industry-leading detection tools to monitor and investigate suspicious bill payment events with 24 x 7 coverage.

Monitoring Services

The core of the FIS Bill Pay Fraud Monitoring Service is a real-time analytics engine that enables FIS to monitor the following bill payment activities while the consumer is interacting with Payment Manager:

- Activity on newly enrolled accounts
- Profile updates
- Payee initiation/maintenance
- Payment initiation/maintenance
- Login/Session monitoring
- Funding account maintenance

Our service uses this information to create a score for each payment transaction based on these and other factors. The fraud-risk score is produced using proprietary prediction algorithms that provide the best "catch-rate" with the lowest false-positive rate. These algorithms are created in an automated, self-training process using real payment and fraud data aggregated over time that allows the system to actively adapt to the changing fraud patterns for maximum accuracy. This allows for the continuous update of models reacting to changing fraud patterns.

If the fraud-risk score for a transaction is high enough to generate an alert, FIS's Digital Payments Fraud Monitoring team analyzes the suspicious activity to determine whether fraudulent activity has occurred. Through the review and analysis of account activity, fraud patterns, and analyst experience, an appropriate decision is made:

- If the suspicious activity is determined not to be fraudulent, no further review is needed and the alert will be closed.

© 2017 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide. This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction or distribution to third parties is strictly prohibited.

- If further information is needed to determine whether the suspicious activity is fraudulent, FIS's Digital Payments Fraud Monitoring team will contact the client for further research (customer contact or review of funding account history) on any alert which is deemed suspicious.
- If the client completes further research and discovers the activity to be fraudulent, the client should block or close the funding account to stop any further activity. The client should immediately notify the FIS Digital Payments Fraud Monitoring team that fraudulent activity has been confirmed so that FIS can ensure the bill pay account has been blocked and they can update the alert history to maintain accuracy of the fraud detection system. If possible, any fraudulent check payments that may have already processed, should have stop payments placed on them.
- If the suspicious activity is determined to be fraudulent by FIS's Digital Payments Fraud Monitoring team, the client will be immediately notified to block or close the funding account and to investigate and stop further activity.

Transaction Suspension

Transaction Suspension is an additional feature available within the fraud monitoring service. With this feature enabled, when a payment is determined to be suspicious by FIS's fraud monitoring processes and it meets criteria established by the FIS Digital Payments Fraud Monitoring team, the payment may be suspended or delayed upon processing until investigation has been completed. The FIS Digital Payments Fraud Monitoring team will research the payment to determine if it is a fraudulent transaction, and then make a decision to release it or cancel it. Payments that qualify for possible suspension will be evaluated as quickly as feasible to minimize consumer impact.

When a transaction is identified as a fraudulent suspect, the FIS Digital Payments Fraud Monitoring team makes every effort to contact our client's fraud team. Transactions can remain suspended up to two business days from when the payment is scheduled to process. In the rare instance where your fraud team does not respond to inquiries from FIS and the chosen action is to automatically release payments, the transaction may be released for processing at the expiration of two business days and any losses occurring as a result will be the responsibility of the client.

When a suspected transaction is confirmed as fraudulent, the FIS Digital Payments Fraud Monitoring team will cancel the payment preventing it from being sent. When a transaction is deemed not fraudulent, the FIS Digital Payments Fraud Monitoring team will release the payment and it will process in the next available processing window.

Not all suspicious payments will be suspended. A suspicious payment will not be suspended if the FIS Digital Payments Fraud Monitoring team is able to complete its research and determine that the payment is not fraudulent prior to the requested processing date of the payment. Additionally, if a suspicious payment does not meet the criteria to be suspended as established by the FIS Digital Payments Fraud Monitoring team, even if the investigation of the payment has not been completed, the payment will not be suspended.

If a payment is suspended because the investigation could not be completed prior to the payment's scheduled processing date, and the payment is subsequently determined to not be fraudulent and released for processing, the payment may be delivered later than the consumer intended. As with other suspended transactions, the consumer will not receive a notification that their payment was suspended.

Client Responsibilities

Successful fraud monitoring and identification requires frequent communication with our clients including e-mails and phone calls. This hands-on communication is particularly warranted when fraud is detected and action is required to stop, block, and report fraud. Our clients' responsibilities include the following actions:

© 2017 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide. This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction or distribution to third parties is strictly prohibited.

- **Alerts –** If a bill payment event triggers a suspicious activity alert, FIS may need more information to determine whether the activity is fraudulent. When FIS notifies your fraud team, you may be required to perform your own investigation or contact your customer directly to confirm the activity.
- **Post-verification –**If FIS has notified you of suspicious or confirmed fraudulent activity, or you have determined suspicious activity is fraudulent, the following steps must be taken by you to prevent additional fraud:
  - Block or close the bill pay and associated funding account.
  - Remove access to Online and Mobile Banking
  - Cancel any bill payments and identify other accounts for your consumer that may have been compromised.
  - Stop payment on fraudulent checks that have not cleared.
  - Recover funds from any processed transactions that are identified as fraudulent.
  - As necessary, work with your impacted consumer and law enforcement.
- **Reporting –** Clients are responsible for filing any required Suspicious Activity Report (SARS) documentation.
- **Other Communication –** Notify FIS's Digital Payments Fraud Monitoring team of any confirmed fraudulent activity so that our fraud monitoring systems can be updated to maintain the highest level of accuracy in our analytical models.

Additional Tools

In addition to the real-time scoring of payment events, FIS uses industry knowledge and experience to create rules that will trigger alerts requiring additional research. FIS has also developed internal databases of known fraud that store consumer and payee information that was related to fraudulent activity. The databases are scanned daily to identify suspicious activity and we will notify our clients of any potential fraud matches.

FIS works diligently to monitor and investigate bill payment activity and identify new trends or schemes in the fraud space leveraging internal monitoring systems, external resources, industry organizations, and subject matter expertise. FIS provides high-quality support services to mitigate fraud in the bill payment space.

For alerts that are identified as fraudulent, FIS may perform additional analysis and actions relative to the case, including but not limited to the following:

- Update the FIS fraud file.
- Perform additional link analysis to determine whether other bill pay accounts have potentially been compromised.
- Close the compromised bill pay account to avoid future fraudulent activity.

Implementation Requirements

A component of the implementation is the exchange of fraud notification contact information between the financial institution and FIS. In addition to sharing contact information for FIS's Digital Payments Fraud

© 2017 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide. This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction or distribution to third parties is strictly prohibited.

Monitoring team and addressing any questions the client may have, the assigned implementation representative will request the following information from the client:

- Contact information for client's fraud management team. A minimum of three contacts is requested. A general "fraud" contact mailbox is preferred with backup contacts via email and phone. When FIS is attempting to notify your designated fraud contacts of suspicious activity, emails will be sent to each contact until an available contact is reached. If a response is not received, we will attempt to reach the contacts again the following day. If the suspicious activity has been determined to be fraudulent by FIS and your designated fraud contacts cannot be reached, FIS may decide to take action on your behalf to prevent further losses.
- Anticipated date the fraud monitoring begins or is turned on. Setup will generally be completed between four and six weeks from the date of the signed contract.

Real-Time Scoring

Real-time scoring provides additional fraud prevention where unique rules are established for high-risk bill payment activity. The real-time scoring engine is tuned to the financial institution's bill payment activity during the first 90 days of bill payment transactions. Fraud monitoring begins immediately upon implementation and the system will achieve optimum scoring of bill pay activity once 90 days of history has been accumulated by the scoring models. During this 90- day period, a higher volume of suspicious alerts may occur until an acceptable history has been established for bill payment accounts.

Currently, fraud monitoring services are not available for PayPal transactions and account-to-account transfers using the Send Money flow in Payment Manager.

Reporting

Standard reports that identify the number of alerts received for suspected fraud and the details of confirmed fraud activity are available in the Customer Service Tool (CST). The below reports are available to clients.

MTD Fraud Alert Volume (FRD-001)

This daily report lists the month-to-date number of alerts by each day of the calendar month. The alerts are broken into the following types:

- Bill Pay
- Enrollment
- Login

MTD Fraud Alert Volume (FRD-004)

The data on this report is the same as the MTD Fraud Alert Volume (FRD-001). This monthly report is created on the third calendar day of each month and contains data from the prior month. New entries are based on the date the alert is initiated.

Fraud Report (FRD-002)

This monthly report lists all alerts marked as fraud. If FIS has collected all data for the fraud case, then the **Case ID**, **Case Name**, and **Case Type** fields are populated. If FIS has not collected this data, then these fields

© 2017 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide. This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction or distribution to third parties is strictly prohibited.

are left blank. This monthly report is created on the third calendar day of each month and contains data from the prior month.

Suspected Fraudulent Transactions Report (SFRD-001)

This daily report gives clients a list of transactions that were suspended as fraud suspects as of the date of the report. It will also show the final decision for any suspect transactions from a previous report. Those transactions will have the date that they were released or declined.

© 2017 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide. This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction or distribution to third parties is strictly prohibited.