



# FraudNet Model Risk Management Governance Report

July 2023



© 2017-2023 Fiserv, Inc. or its affiliates. All rights reserved. This work is confidential and its use is strictly limited. Use is permitted only in accordance with the terms of the agreement under which it was furnished. Any other use, duplication, or dissemination without the prior written consent of Fiserv, Inc. or its affiliates is strictly prohibited. The information contained herein is subject to change without notice. Except as specified by the agreement under which the materials are furnished, Fiserv, Inc. and its affiliates do not accept any liabilities with respect to the information contained herein and are not responsible for any direct, indirect, special, consequential or exemplary damages resulting from the use of this information. No warranties, either express or implied, are granted or extended by this document.

<http://www.fiserv.com>

Fiserv is a registered trademark of Fiserv, Inc.

Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Document Version 1.11  
Revised July 2023  
Revised April 2023  
Revised January 2023  
Revised October 2022  
Revised July 2022  
Revised April 2022  
Revised January 2022  
Revised October 2021  
Revised July 2021  
Revised February 2021  
Revised October 2020  
Revised May 2020  
Revised November 2019  
Revised March 2019  
Revised August 2018  
Published December 2017

# Contents

<b>About This Document .....</b>	<b>v</b>
Purpose .....	v
Audience.....	v
Scope .....	v
<b>Chapter 1: FraudNet.....</b>	<b>1</b>
Terminology .....	1
Fraud Model Analysis and Testing Methodology .....	1
Fraud Characteristics and Their Evaluation .....	1
Sampling Method for Model Development .....	2
Data Control and Validation.....	2
Logistic Model.....	2
Fraud Model Overview .....	3
Model Performance Validation (Q1 2022) .....	5
Alerts .....	9
Behavioral Rules.....	9
Negative List Rules .....	10
Alerts Not Associated with Rules .....	10
FraudNet Rule Configurations .....	10
FraudNet IP Geolocation .....	10
IP Geolocation Information Bar.....	10
Subscriber IP Profile .....	11
Geolocation Detection Rules .....	11
Client Communication .....	12
<b>Chapter 2: CheckFree RXP-Popmoney Transaction Monitoring .....</b>	<b>13</b>
CheckFree RXP-Popmoney Fraud Monitoring .....	13
Velocity Rules .....	14
CheckFree RXP-Popmoney Account Information .....	14
<b>Chapter 3: Best Practices .....</b>	<b>15</b>
Investigation Policy.....	16
Processing Guidelines.....	16
Overnight Payments.....	16
Payments Held by FraudNet Past the Subscriber's Requested Payment Due Date.....	17
Same Day Payments .....	17

<b>Chapter 4: Operational Procedures .....</b>	<b>18</b>
Logging In to the FraudNet Alert Manager .....	18
Assigning Cases .....	18
Accessing Alerts.....	19
Searching for an Alert.....	20
Accessing Subscriber Transaction History .....	21
Linking Non-Alerted Transactions.....	21
Updating Negative Lists Through the Transaction History .....	22
Viewing a Transaction in PartnerCare .....	22
Updating a Case .....	23
Updating a Case for Confirmed Fraud .....	23
Updating a Case to Release a Transaction.....	25
Manual Alerts .....	26
Creating Manual Alerts.....	26
Working a Manual Alert.....	26
Marking an Alert for Follow Up.....	26
Viewing the Associated Case .....	27
Viewing an Alert's Historical Log.....	28
Printing Alert Details .....	28
Using Link Analysis Functions .....	29
Working a Popmoney Confirmed Fraud .....	30
FraudNet.....	30
Compass Restricted Hold / Suspension Procedures .....	31
Working a Suspicious Transaction Alert.....	32

## About This Document

This section provides information about this document, including:

- Purpose
- Audience
- Scope

### Purpose

This document describes the FraudNet Engine and FraudNet Alert Manager from Fiserv.

### Audience

The audience for this document includes fraud specialists and case distribution managers. Fraud specialists include fraud specialists and investigators with both Fiserv and sponsors who use FraudNet.

### Scope

The scope of this document includes limited information about the FraudNet Engine and FraudNet Alert Manager. Information about fraudulent activity in general is beyond the scope of this document.

# Chapter 1: FraudNet

FraudNet™ from Fiserv is a system that brings together a network of fraud professionals from multiple financial institutions to combine efforts to deter electronic bill payment fraud. By using a common interface and detection tool, the system grows stronger with each alert associated with a confirmed case of fraud.

The FraudNet Alert Manager is the network interface and main junction for all clients using FraudNet.

The FraudNet Engine is the detection tool that automatically detects and prevents suspicious payment activity. All Bill Pay payment activity is assessed, and if predetermined threshold scores are reached, the FraudNet Engine holds the payment and generates an alert for investigation by fraud specialists. Using the FraudNet Engine improves efficiency in detection and reduces the costs due to fraudulent activity.

## Terminology

The following terminology is used in the Alert Manager for fraud types.

Term	Definition
Account Takeover	Third party fraud where an unauthorized user has access to a consumer's bill payment account and attempted to move money out of the bank account.
ID Theft	An account was created using a false/fake identity and the same identity was utilized on the funding account.
Bank Fraud	A funding account was under the name of another individual or business.
ID Theft / Bank Fraud	Combination of ID Theft and Bank Fraud. An account was created using a false/fake identity. Subsequently, the funding source was under the name of another individual or business.
Electronic Kiting	First party fraud where the account holder was attempting to move money via bill payment, account-to-account transfer, or person-to-person payment when the source account was not adequately funded.
Friendly Fraud	A relative or friend accessed the consumer's bill payment account without authorization and attempted or succeeded to transmit funds.
Pay Scheme Victim	A consumer claims that he or she is a victim of a payment fraud scheme (for example, grandchild ransom scheme, elder fraud, or fake charity).

## Fraud Model Analysis and Testing Methodology

The underlying engine for FraudNet consists of a logistic model using the framework and methods suggested in *Applied Logistic Regression* by David W. Hosmer and Stanley Lemeshow (Wiley, 1989). Two other publications providing primary support in the development of the latest version of the FraudNet engine are *Applied Multivariate Statistical Analysis* by Richard A. Johnson and Dean W. Wichern and *Statistical Inference* by George Casella and Roger L. Berger.

This method for modeling dichotomous variables is a standard practice in many areas of financial matters (for example, modeling whether a transaction is fraudulent or not).

## Fraud Characteristics and Their Evaluation

Through input from several different areas within Fiserv (including Fiserv's team of ACFE certified fraud subject matter experts), a number of financial behaviors, subscriber profile features, and transaction characteristics were identified as candidate exogenous variables for inclusion in the engine's model.

Using a variety of transformations, these factors were individually subjected to a bivariate analysis with relation to the target variable for indicating fraud. These bivariate analyses included, among other measures, the information value (IV). Binning modes and distributional aspects were considered in the evaluation.

## Sampling Method for Model Development

A four-month transaction sample was used in the development phase of model construction, and a more recent four-month sample was used to validate the model (the two samples were mutually exclusive sets). In-time sampling of both datasets was considered, but the time to implementation was a consideration and fraud behavior evolves quickly. This type of hold-out sample validation allows for the nearest-term evaluation of the model's capabilities prior to implementation. Subsequent updates and validations follow this pattern.

Each sample consists of all detected fraud transactions, transactions linked to those transactions, and all false positives, as well as a 1-in-20 sampling of transactions not tagged for fraud.

Missing values are treated as their own separate informative "range" of value for the variable, receiving weighting according to how all weights are assigned in the model. After estimation, and during review of the model, weights for missing value states are evaluated for logical soundness with respect to other weights for values within the range of the variable of interest.

## Data Control and Validation

Data elements within the transaction record samples derive from tables within Fiserv's mainframe database and from the FraudNet alert database. Both environments are maintained and administered by Fiserv's Enterprise Technology Group.

Samples are extracted using standard test scripts. Randomized subsamples are compared with system records to ensure data integrity.

All data elements in each sample are validated via additional scripting that checks distribution metrics for continuous variables and frequency distributions for discrete-valued variables.

## Logistic Model

A randomized selection using best subsets selection and stepwise selection was used for evaluating the main factors. With a pool of best subsets of main factors, further explorations of interactions were conducted. Model performance was evaluated based on standard metrics such as the area under the curve (AUC), the Gini coefficient, the Kolmogorov–Smirnov test, and adherence of actual log odds to predicted values.

To balance detection with queue volumes, false positive rates and false negative rates were also determined at various thresholds.

In the development of the FraudNet model, over 100 raw variables were considered. Derived variables, reflecting transformations and interactions among the initial 100 raw variables, increased the cardinality of the original set to over 200 variables. These variables were the focus of consideration through input from numerous internal teams, as well as industry research.

To winnow the set of variables to a reasonable selection, each variable was reviewed for its capacity to separate the dependent variable's values into two distinct, mono-valued classes. This was accomplished in these ways:

1. Overlaps in the distributions of the "bad" population and the "good" population, with respect to the candidate variable's range, were measured. High levels of overlap disqualified a candidate variable.
2. The IV measure with respect to numerous binning scenarios was recorded for each variable. A binning search routine was developed for achieving optimality in IV while maintaining balance between over-discretization and parsimony.

3. Candidates were tested using best subsets and stepwise selections in the SAS logistic procedure. With an optimal additive model selected, all interactions were likewise tested for significance, and a final model was proposed.

To evaluate a final proposed model, comparison runs on the validation sample against the current champion model were performed. ROC curves were compared and “bad” capture rates for various percentiles in the score band were calculated and compared among the models for consideration and the champion.

## Fraud Model Overview

For each payment, the system determines a fraud score. The FraudNet base model is a straightforward, additive scoring model; the engine checks for various fraud cues, and for each cue, a fixed number of points is added to the fraud score.

The FraudNet default alert threshold is 40 points. If a transaction crosses the alert threshold, the payment is placed on hold and an alert is generated in the FraudNet Alert Manager. At this threshold, a financial institution might expect an alert ratio of approximately 1,500 to 1 (1,500 transactions to 1 alert). Customized and autonomous rules can affect the alert ratio.

There are four basic components of the overall fraud model:

- FraudNet Base Model
  - The logistic model as described above. These are a series of individual variables with positive and negative weighting values.
- Autonomous Rules
  - Combinations of variables that form independent rules based on actual fraud events and trends. Scores for these rules are added after the model evaluation. Most autonomous rules have a high score value to ensure that an alert will be generated. For example, if an autonomous rule applies, the autonomous rule’s score will be added to the base model score to force an alert to be generated (i.e., to push the score over the alert threshold). For more information, see “Behavioral Rules” on page 9.
- FraudNet Negative Files
  - Collection of confirmed fraud data gathered from all participating FraudNet financial institutions:
    - Routing and account number pairs for funding accounts
    - Full email address
      - Disposable email address domains
    - Victim and suspect Social Security numbers
    - Payee account numbers
    - Eleven-digit remittance ZIP Code for unmanaged payees
    - IP addresses
- IP Geolocation
  - CheckFree® RXP® collects the IP address associated with each transaction. This address is used to approximate the origination point of the transaction and can be used to generate alerts. For more information, see “FraudNet IP Geolocation” on page 10.



The fraud scoring in the current model proceeds in three stages:

1. The engine checks for various fraud cues (see table below). Fraud cues are independent and combined variables that make up the scoring attributes of the FraudNet base model. For each cue, a fixed number of points is added to the fraud score. The output of this stage is the raw fraud score.
2. The raw fraud score is used to determine the *probability* that the payment is fraudulent.
3. The *probability* of fraud is multiplied by the payment amount to give the *expected fraud value* (EFV). The EFV reflects not only the probability that a payment is fraudulent, but also the amount of the payment. A large payment may generate a high value even if the probability of fraud is low.

- $EFV = (\text{fraud probability}) \times (\text{payment amount})$

Fraud Cue	Definition
Managed Payee	Indicates that the payee or biller has an electronic agreement in place with Fiserv. The payment will be sent to the known biller address in the Fiserv system. Remit Center number is greater than 0.
Familiar Payee	This subscriber has paid this payee before, and at least one prior payment processed with a <i>due date</i> at least 27 days before the <i>current date</i> of the current payment (i.e., the date when the current payment is processed for fraud).
Age of Payee	Difference between the time the subscriber added the payee and when the subscriber scheduled the payment.
Subscriber Business Type	Subscriber type is <i>business</i> , rather than <i>individual</i> .
Subscriber Profile Age	Difference between the timestamp of the subscriber's enrollment and when the subscriber scheduled the payment.
Subscriber's Local Time (Hour)	Derived variable that measures the time of day that the user was (in-session) using the Bill Pay product.
Amount	Amount of the payment.
Round Dollar Amount	Amount of the payment contains zero cents (.00), which can be an indicator of fraud.
[QH] (quick hitter)	Velocity Rule: Provides unit and cumulative dollar counts of payments to a single payee in a given time frame.
Recent Email Address Maintenance	Time of the most recent change to the subscriber's email. Utilizes timestamps (add date vs. maintenance date) within the Fiserv maintenance logs.
[BUST] (payee is near subscriber)	Unmanaged payment rule measures distance of locally based payments using ZIP distance data. This rule also considers how recently the payee was added.
[BUS2] (payee is far from subscriber)	Unmanaged payment rule measures distance of non-locally based payments using ZIP distance data. This rule also considers how recently the payee was added.

## Model Performance Validation (Q1 2023)

The following performance validation uses a payment sample from Q1 2023. It contains all alerted payments and 1 out of every 20 non-alerted payments.

- Fraud data sample range: January 2023 through March 2023
- Number of observations (transactions): 4,464,853
- Number of fraud cases: 8,930

ROC (receiver operating characteristic curves) measure how well the model can separate positive events (fraud) and negative events (non-fraud). A highly efficient model would produce a high true positive rate (TPR) and a low false positive rate (FPR). Figure 1 shows the comparison of ROC curves for the base model and overall score. The overall score is the combination of the base model and the autonomous rule scores.

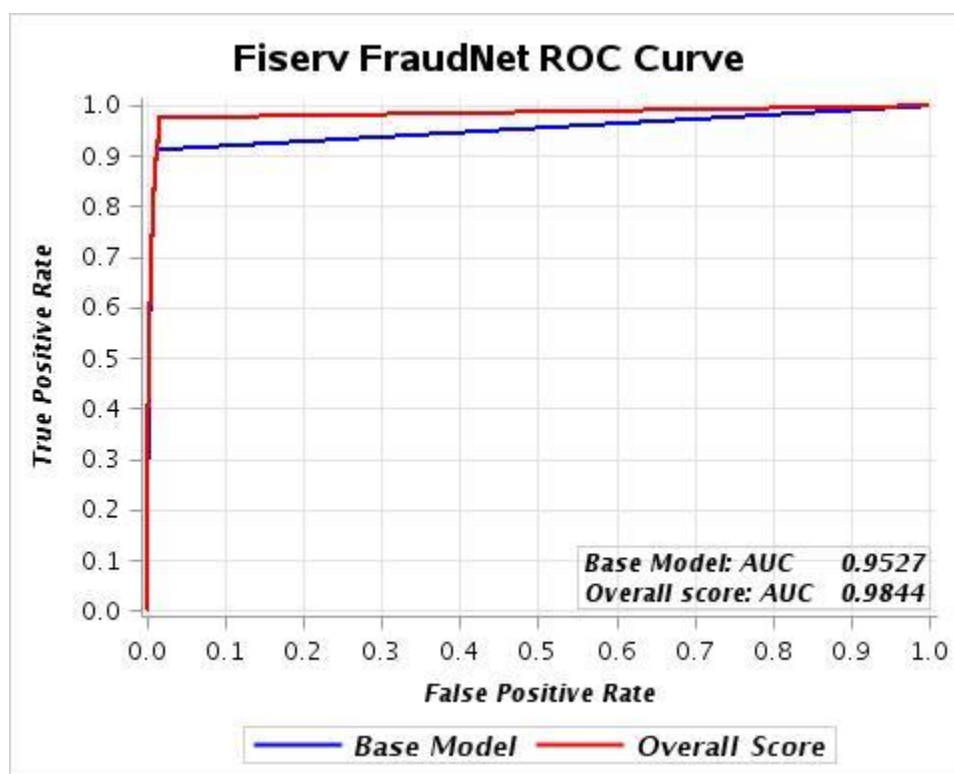


Figure 1 FraudNet ROC for the Base Model and Overall Score

It is important to note that compared to the base model score, the overall score has gained another significant lift. The statistical base model detects 95.2% of all fraud, whereas the overall model leverages fraudulent activities across the network of FraudNet clients and improves the detection rate to 98.4%.

The Gains chart compares the cumulative percentage of fraud with the cumulative percentage of all transactions. Figure 2 shows the Gains chart for the overall score. For example, less than 2% of the total transactions with the highest predicted probability contain approximately 95% of the total fraud.

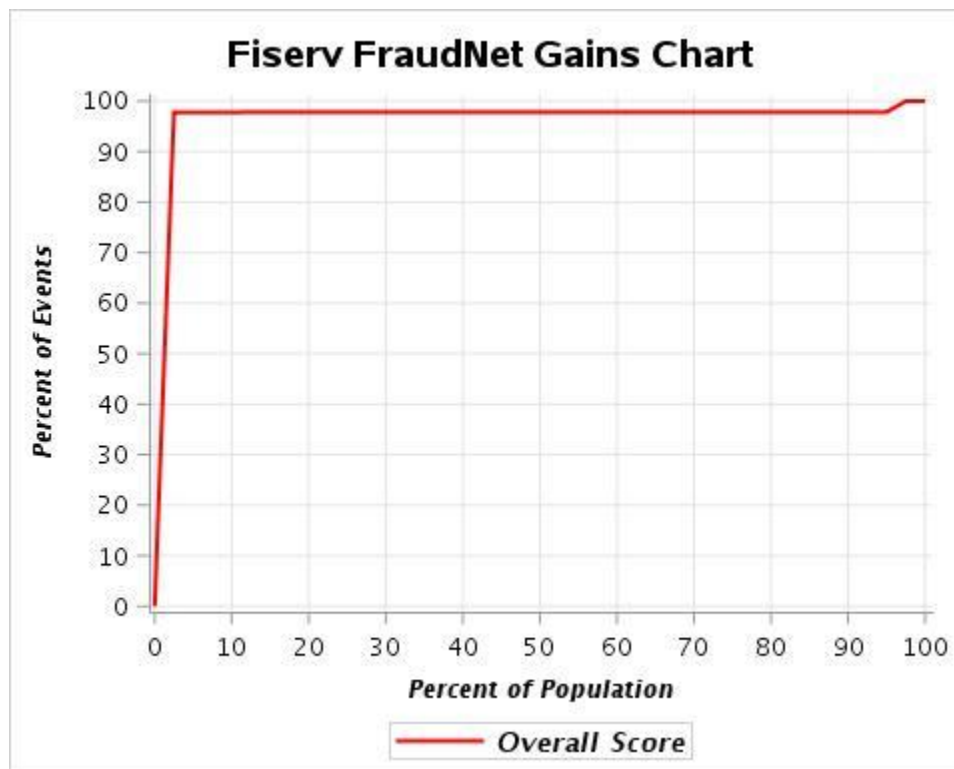


Figure 2 FraudNet Gains Chart for the Overall Score

Table 1 displays fraud detection rates for the theoretical alert thresholds. This table lists the specific points along the ROC with the corresponding model classification performance (TPR and FPR) depicted in Figure 1.

Example: Alert threshold = 50 and total number of transactions = 4,464,853

- 8,452 payments alerted and were found to be fraudulent. True Positive Rate:  $TP/(TP + FN) = 94.65\%$
- 67,635 payments alerted but were confirmed to be valid. False Positive Rate:  $FP/(FP + TN) = 1.52\%$
- Approximately 4.4 million payments did not alert and were valid.

Alert Threshold	True Positive (TP)	False Positive (FP)	TP Rate (detection rate)	FP Rate
50	8,452	67,635	94.65%	1.52%
100	6,918	33,729	77.47%	0.76%
150	6,250	25,750	69.99%	0.58%
200	5,732	20,957	64.19%	0.47%
250	5,415	18,334	60.64%	0.41%
300	5,095	16,072	57.05%	0.36%
350	4,848	14,466	54.29%	0.32%
400	4,653	13,027	52.11%	0.29%
450	4,491	12,104	50.29%	0.27%
500	4,304	11,275	48.20%	0.25%
550	4,210	10,619	47.14%	0.24%
600	4,120	10,112	46.14%	0.23%
650	4,049	9,504	45.34%	0.21%
700	3,962	9,106	44.37%	0.20%
750	3,903	8,666	43.71%	0.19%
800	3,818	8,310	42.75%	0.19%
850	3,771	7,996	42.23%	0.18%
900	3,711	7,721	41.56%	0.17%
950	3,672	7,405	41.12%	0.17%
1000	3,597	7,013	40.28%	0.16%

**Table 1. Fraud Detection for Alert Threshold 50–1,000**

Table 2 is a breakout of alert thresholds equal to or below 50. The alert threshold is selected to obtain the optimal balance between the high fraud detection rate and the capacity of operations required to work the alerts.

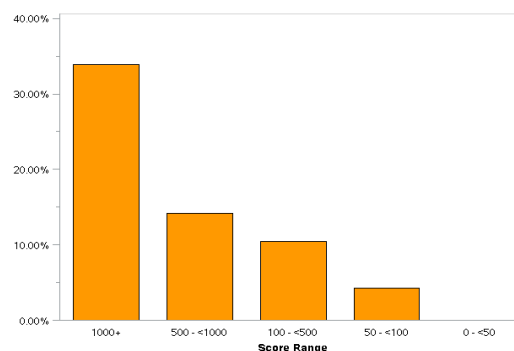
Overall Score				
Alert Threshold	True Positive (TP)	False Positive (FP)	TP Rate (detection rate)	FP rate
10	8,727	76,421	97.73%	1.72%
20	8,725	74,741	97.70%	1.68%
30	8,701	73,419	97.44%	1.65%
40	8,666	72,659	97.04%	1.63%
50	8,452	67,635	94.65%	1.52%

**Table 2. Fraud Detection for Alert Threshold 10–50**

Table 3 and Figure 3 show the percentage of fraudulent payments within each score range.

**Fraud Rate in Each Score Range**

Score Range	Fraud	No Fraud*	Fraud Rate in Score Range
1000+	3,597	7,013	33.90%
500 - <1000	707	4,262	14.23%
100 - <500	2,614	22,454	10.43%
50 - <100	1,534	33,906	4.33%
0 - <50	478	4,388,288	0.01%
Total	8,930	4,455,923	0.20%



**Table 3 and Figure 3. Fraud Rate in Each Score Range**

\*Only 1 out of every 20 non-alerted payments are captured in the sample data and stored. Therefore, the actual fraud rate in each score range is lower than the rates shown in the sample.

## Alerts

Payments that cross the alert score threshold generate alerts.

- Payments are prevented from processing in the payment system until they are either rejected as fraud or released as valid through the FraudNet Alert Manager.
- FraudNet automatically sends all alert notes to cases within PartnerCare.
- There is a mnemonic or acronym for every rule to show why an alert was generated. Only autonomous rules and base model rules have mnemonics; individual scoring variables in the base model do not.
- All alerts are available in the FraudNet Alert Manager within 15 minutes of a payment being scheduled.

## Behavioral Rules

The following table contains the current rules that can trigger an alert; these values are subject to change.

Rule	Mnemonic	Definition
Subscriber Info Change	ACHG	The subscriber's email address has changed recently.
Account Transfer Sleeper	A2AS	Monitors for newly created transactions being scheduled on a previously dormant account.
Bank by Mail	BBM	Monitors transactions being remitted directly to financial institution branches for deposit into a checking account.
Bust-Out	BUST	The subscriber is attempting to make a payment to a recently added payee and the payee's address is located near the subscriber's address.
Bust-Out II	BUS2	The subscriber is attempting to make a payment to a recently added payee and the payee's address is located far from the subscriber's address.
DDA = Payee Account#	EKITE PKITE	Monitors for transactions where the funding account matches the receiving or payee account number. This rule monitors both electronic and paper transactions.
Managed Velocity Payment	MVP	This is an optional rule used to monitor the velocity of payments within a particular industry or set of industries. Contact your assigned Fraud Specialist to establish the thresholds for this velocity rule.
Payment Type Rule	PTAR	Targets a specific payment type; e.g., overnight check or bill payment. Rule can be configured by amount.
Quick Hitter	QH	Multiple payments have been made to a newly added payee.
Specific Remittance Rule	SRR	Monitors a specific electronic merchant in the bill payment system. Dollar amount thresholds can be set to limit false alert rates or target specific dollar ranges.
Unmanaged Velocity	UNM_VP	Monitors the velocity of unmanaged payments on an individual subscriber's account. This rule can also be used to target lower-dollar high-risk unmanaged payments.
A2A Velocity	VELTRAN	Monitors the velocity of account-to-account transfers being made by a specific subscriber.

## Negative List Rules

Rule	Mnemonic	Definition
Negative List - DDA	NLD	The subscriber's bank account number is on a list of bank accounts associated with past confirmed cases of fraud.
Negative List - Email	NLE	The subscriber's email address is on a list of email addresses associated with past confirmed cases of fraud.
Negative List - Payee Account #	NLP	The subscriber's account number with the payee is on a list of payee account numbers associated with past confirmed cases of fraud.
Negative List - SSN	NLS	The subscriber's Social Security number is on a list of Social Security numbers associated with past confirmed cases of fraud. Note: NLS is not currently active.
Negative List - 11-digit ZIP	NLZ	The payee's 11-digit ZIP Code is on a list of payee address ZIP Codes linked to past confirmed cases of fraud.

## Alerts Not Associated with Rules

The following table contains alerts that are not associated with rules; these values are subject to change.

Alert Type	Mnemonic	Definition
Manual Alert	MA	Externally reported fraud that FraudNet missed or that failed to trigger an alert. Generated by the client to notify Fiserv of the missed data. It is crucial that these accounts be entered into the system so that a fraud analyst can track and modify client scoring parameters in the event their detection statistics begin to drop.

## FraudNet Rule Configurations

Each of the rules listed above can be customized for sponsors in individual business units. Sponsors who elect for Risk Assist, where FraudNet alerts are managed by Fiserv, typically are not assigned to individual business units and will use FraudNet default rules.

## FraudNet IP Geolocation

FraudNet pulls the IP address associated with a payment scheduled through CheckFree RXP to determine an approximate point-of-origin for where the payment was scheduled. Additional fields can be utilized in rules outlined in "Geolocation Detection Rules" on page 11 (e.g., carrier, anonymizer status, etc.).

## IP Geolocation Information Bar

The FraudNet Alert Manager contains geolocation information in the Alert Details page. When FraudNet receives a subscriber's IP address for a scheduled transaction, information displayed includes the geographic information, carrier, ASN, and Anonymizer Status. A confidence score is shown next to the subscriber's country, state, and city. The higher the confidence score, the more likely the transaction was scheduled from that location.

IP Geolocation		<a href="#">Subscriber IP Profile</a>	
IP Address:	120.43.21.32	Country (86%):	cn
Carrier:	chinanet	State (73%):	fujian
ASN:	4134	City (51%):	fuzhou
		Anonymizer Status:	-
		Continent:	asia

Within the IP Geolocation Information Bar, the following definitions apply:

**Anonymizer Status:** Indicates whether the IP address is associated with a known anonymous proxy where Internet activity is untraceable.

**ASN** (Autonomous System Number): Globally unique number assigned to a single network or a group of networks that is administered by a single administrative entity. This is not used currently in the FraudNet detection strategy.

**Carrier:** The name of the organization that owns the ASN.

## Subscriber IP Profile

As agents mark alerts as No Fraud, the associated IP address is added to the Subscriber IP Profile. Subsequent transactions scheduled from an IP address on that subscriber's IP profile will be scored accordingly to reduce false positives.

The Subscriber IP Profile holds up to five IP addresses at a time. Older IP addresses may need to be deleted to add more up-to-date data to the profile. Agents must thoroughly investigate IP addresses and take note of which IP addresses are most frequently used by a subscriber. Transaction counts are included in the profile.

To manually add an IP address to a subscriber's IP profile, click **Add to Profile**. To delete an IP address from a subscriber's profile, click **Remove from Profile**.

Subscriber IP Profile				
To add the IP address associated with the current alert, select the 'Add to Profile' link below.				
<b>Name:</b> KASIM DIN	<b>Subscriber ID:</b> 01160002006	<b>Sponsor ID:</b> 25725		
IP Address	Last Access Date	Access Count	Profile	
127.0.0.1	Current	-	<a href="#">Add to Profile</a>	

## Geolocation Detection Rules

Rule	Mnemonic	Definition
Negative Anonymizer Status	NLAS	Monitors for active or private anonymizers.
Negative Country Code	NLCN	Monitors for hot-listed countries by country code.
Negative IP Carriers	NLIC	The carrier has been identified as high risk.
Negative IP Address List	NLIP	The subscriber's IP address is associated with confirmed fraud activity.
Out-of-State IP	NSIP	Calculates mileage between the subscriber's address and the latitude/longitude of the IP origination point. <b>Note:</b> Rule applies only to IPs in a state other than the subscriber's address.



As with other negative data, IP addresses can be added to the shared negative lists from the FraudNet Alert Manager. To reduce false positives, all IP addresses should be thoroughly screened before adding them to the negative list.

**Note:**

Do not add any IP address in the following categories:

- Mobile
- Private (IPs between 10.0.0.0 – 10.255.255.255)
- Publicly accessible IPs (business hotspots)

Negative lists for countries, carriers, and anonymizer statuses are managed only by Fiserv. Clients can submit requests for additions to these three lists to their assigned Fraud Investigator. To control false positives, all suggestions from clients undergo a secondary evaluation to determine if the data is a viable addition to the negative lists.

## Client Communication

When notified of unauthorized transactions or when payments have been processed without being suspended by FraudNet, clients should follow the procedures in this section based on the payment method type: laser drafts, corporate checks, or electronic payments.

### Laser Drafts (Code 03)

Because a laser draft is processed just like a personal check against a subscriber's account, the client has full return and stop payment responsibilities.

### Corporate Checks (Code 02)

If a subscriber reports that a payment was unauthorized within the NACHA guidelines:

1. The client should contact Fiserv Fraud Control or Client Services Support to request that a stop payment be placed on the corporate check.
2. Fiserv will return all debits within three business days of the stop payment order.

If the corporate check clears before the requested stop payment order is placed, Fiserv can attempt to initiate a check return request if Fiserv is notified within 24 hours of the clearing date. Any returned funds can be settled with the client.

### Electronic Payments (Codes 19 and Higher)

If a subscriber reports an unauthorized transaction that originated through the online banking service, the client should not immediately return that transaction as an unauthorized transaction.

Instead, the client should contact Fiserv to validate the transaction and have a Fiserv Fraud Investigator assist in recovery efforts with the merchants.

**Note**

If Fiserv is not the responsible party for initial/recurring authentication, the client should not return any payments that originated via the online banking service to Fiserv.

## Chapter 2: CheckFree RXP-Popmoney Transaction Monitoring

This section applies only to clients who migrated from legacy ZashPay to the Popmoney platform.

### CheckFree RXP-Popmoney Fraud Monitoring

Fraud monitoring of Popmoney payments uses a set of standardized proprietary velocity rules and hotlists to detect potentially fraudulent activity. Below are the rule indicators and descriptions of the various negative files used for fraud monitoring list matching.

#### Note

Even though Popmoney transactions may be managed through the FraudNet Alert Manager, payments are scored through a different fraud engine. Neither the FraudNet model nor the FraudNet rules apply to Popmoney transactions.

Negative List Match	Mnemonic	Definition
CENET Sender SSN Match	CNT1	Matches the consumer's SSN to a list of established suspect and victim Social Security numbers on the CENET negative lists.
CENET Non-Host Routing Number Match	CNT2	Matches the bank routing number to an established list of routing numbers known to have high volumes of fraud or tied to prepaid and stored value cards on the CENET negative lists.
CENET Receiver Routing + Non-Host Account Match	CNT3	Matches the receiving DDA and RTN combination to a list of known suspect and victim accounts on the CENET negative lists.
CENET Sender Registered Phone Number Match	CNT4	Matches the sender's contact information to a list of known or reported suspect phone numbers on the CENET negative lists.
CENET Sender Registered Email Match	CNT5	Matches the sender's email address with a list of known or reported email addresses linked to fraudulent activity CENET negative lists.
CENET Sender IP Address Match	CNT6	Matches the sender's Internet Protocol address to a list of suspect IP addresses.
To Source Bank Account Match	FNT1	Matches the source DDA or receiver bank account with the FraudNet RTN DDA negative lists.
From Source Bank Account Match	FNT2	Matches the source or sender bank account with the FraudNet RTN DDA negative lists.
Payee Email Address Match	FNT4	Matches the sender's email address with a list of known fraudulent email addresses in the FraudNet negative files.
Payee TID or Social Security Number Match	FNT5	Matches the consumer's SSN to a list of established suspect and victim Social Security Numbers on the FraudNet negative lists.
IP Address	FNT6	Matches the sender's Internet Protocol address to a list of suspect IP addresses.
Negative Country List	FNT7	Triggers an alert when an IP address is linked with a country that has been blocked in the bill payment and Popmoney networks.

These lists are supplemented with data from fraudulent activity detected within the Fiserv bill payment and Popmoney network. Violations or positive hits on any of the triggers in the fraud system generate an alert in the FraudNet Alert Manager.

## Velocity Rules

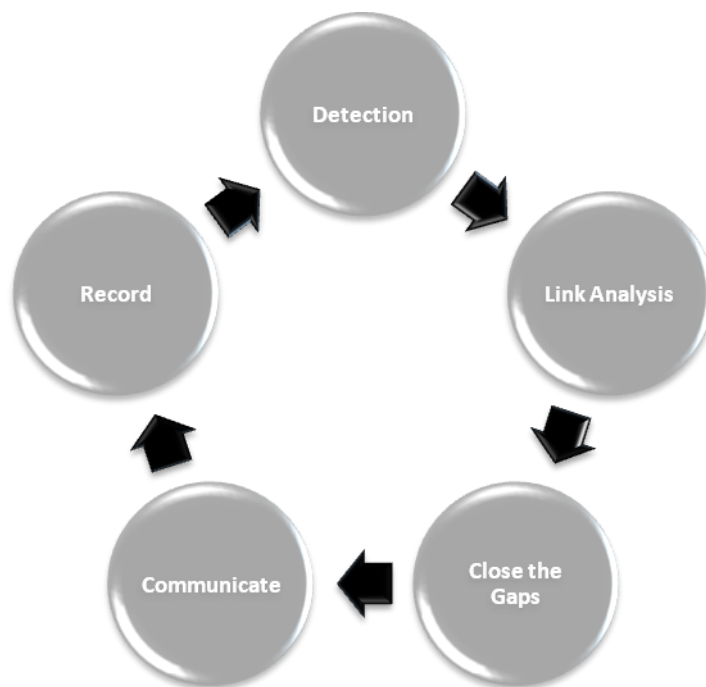
Velocity Rule	Mnemonic	Definition
Personal Payment Receiver Velocity	Z016	Measures velocity of transactions and cumulative dollar amounts being received by an individual. Clients subscribing to Popmoney should work with their Fraud Specialist to establish the appropriate velocity and amount thresholds.
Personal Payment Sender Velocity	Z001 – Z015	Measures velocity of transactions and cumulative dollar amounts being sent by an individual. Clients subscribing to Popmoney should work with their Fraud Specialist to establish the appropriate velocity and amount thresholds.
High Risk ABA	Z041	Certain routing numbers are marked as high risk in the Popmoney system.
Transfer Foreign Country	Z042	Transfer from a foreign country.
IP Routing Type	Z043	
Multifactor Trigger	Z_RF1_RF2	<p>Rules created using this methodology are displayed using multiple instances of an abbreviation appended with a level number indicating the level from low {0} to high {5} for the attribute.</p> <p>Abbreviations:</p> <ul style="list-style-type: none"> <li>AB - List of ABA numbers</li> <li>AG - Age of the profile in the system</li> <li>CTY - List of med-high risk foreign countries</li> <li>EM - Changes in email/contact information (how recent)</li> <li>EPH - User sending transfer to an email or phone contact</li> <li>IP - Geolocation information (including distance/type)</li> <li>KTP - User sending transfer to a DDA for deposit</li> <li>PH - Changes in phone contact Information (how recent)</li> <li>TK - Contact token usage and age information</li> <li>UT - Utilization of the target account/ token</li> <li>VL - Cumulative transfers from/to account in a period of time (velocity)</li> </ul> <p>For example, Z002_EPH_TK0_UT3_IPM indicates that there were transfers sent to an email/phone contact that was registered recently, with medium utilization, showing a higher risk factor for geolocation properties (Mobile).</p>

## CheckFree RXP-Popmoney Account Information

FraudNet clients must use Compass to access and view Popmoney transactions and accounts. Compass is accessible through PartnerCare and uses your existing PartnerCare credentials. Please reference the Compass user guide for more detailed information on Compass functionality.

## Chapter 3: Best Practices

Fiserv uses this methodology when investigating fraud alerts or externally reported fraud claims:



### Detection

- FraudNet system detects suspicious payments utilizing cues and rules described on previous pages.

### Link Analysis

- A crucial part of investigating fraud occurrences is using link analysis to link accounts, email addresses, payee information, and other applicable attributes and data points to the current fraud trend or attack under investigation.

### Close the Gaps

- Secure all accounts discovered by the link analysis:
  - Freeze or close accounts.
  - Cancel payments and stop checks where applicable.

### Communication

- Contact linked merchants/billers, financial institutions, and consumers (if appropriate) that are linked to the case.

- Proliferate information about the fraudulent activity to all applicable parties including:
  - Risk Analytics (for Fiserv associates only)
  - Fiserv associates: Notify clients as needed
  - FraudNet clients: Contact the assigned fraud investigator at Fiserv as needed

## Record the Data

- Enter Manual Alerts into the FraudNet Alert Manager for all fraudulent payments that did not alert—and also—were not able to be linked to the alerted “parent” transaction. Without data about fraudulent payments missed by the engine, strategy adjustments are not possible since detection rates would consistently report at 100%.

## Investigation Policy

All alerts must be worked before the close of business on the day of the alert. If a fraud specialist is unable to determine if the alerted payment is valid or fraudulent, they should contact the:

- Subscriber to verify a payment if, and only if, the contact information can be confirmed and validated.
  - Fiserv associates: Follow all internal procedures regarding contact based upon client-specific procedures. The client should be contacted to verify either the subscriber contact information or the validity of the payment.
- Merchant/Biller to confirm account information (if applicable and appropriate).

It is recommended that alerts be sorted by payment due date. The FraudNet Alert Manager automatically sorts payments based on the earliest due date. Payments with next day due dates should be worked first and released before 5 p.m. ET to ensure timely processing.

It is not recommended to hold alerts more than 48 hours from the alert timestamp.

## Processing Guidelines

### Overnight Payments

If an overnight payment alerted in the system and was scheduled the same day it alerted, to make sure it processes as an overnight it would need to be released before 4 p.m. that same day; otherwise, it will process in the next day's window.

### Use Cases

1. On June 10, a consumer schedules an overnight payment at noon. The payment alerts in FraudNet at 12:15 p.m. on June 10. A fraud specialist releases the payment at 1:30 p.m. on June 10. The payment is processed as an overnight payment with a delivery date of June 11.
2. On June 10, a consumer schedules an overnight payment at noon. The payment alerts in FraudNet at 12:15 p.m. on June 10. A fraud specialist releases the payment at 4:15 p.m. on June 10. The payment is not processed as an overnight payment and falls to the 4 p.m. processing cutoff window on June 11 with a delivery date of June 12.

## **Payments Held by FraudNet Past the Subscriber's Requested Payment Due Date**

When an investigator releases a transaction that has been held past a subscriber's intended payment date, that transaction will not be processed until the next day's cutoff time. Alerted payments will not process at all if held 10 calendar days from the due date.

The CheckFree Guarantee does apply to legitimate transactions that have been held by specialists past the subscriber's due date. These claims are handled by customer solutions at Fiserv and should be routed utilizing Sponsor Care / PartnerCare. Fraud Control at Fiserv does not process late fee claims.

## **Same Day Payments**

Same day payments are processed using a preauthorization check against the FraudNet negative files and are evaluated against the FraudNet payment model after they have already processed. As such, these payments are not prevented from processing even if they generate an alert in the Alert Manager.

If fraud is confirmed on a same day payment, it is advised to alert the biller as quickly as possible to attempt to prevent the credit from applying to the intended account.

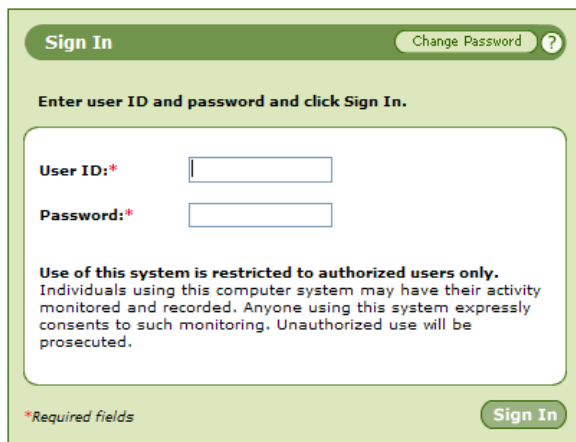
## Chapter 4: Operational Procedures

This chapter contains walkthroughs of common procedures and includes a process flow for working a confirmed fraud case.

### Logging In to the FraudNet Alert Manager

The FraudNet Alert Manager is part of the PartnerCare system. The same credentials used to access PartnerCare also access the FraudNet Alert Manager (see the login screen below).

Access to PartnerCare and FraudNet is managed by locally-designated PartnerCare administrators.



The sign-in screen features a green header with 'Sign In' and 'Change Password' links. Below is a prompt to enter user ID and password. Two input fields are provided, with the first labeled 'User ID: \*' and the second 'Password: \*'. A disclaimer states that system use is restricted to authorized users and that activity is monitored. A 'Sign In' button is at the bottom right, and a note indicates that fields with an asterisk are required.

**Sign In** [Change Password](#) ?

Enter user ID and password and click Sign In.

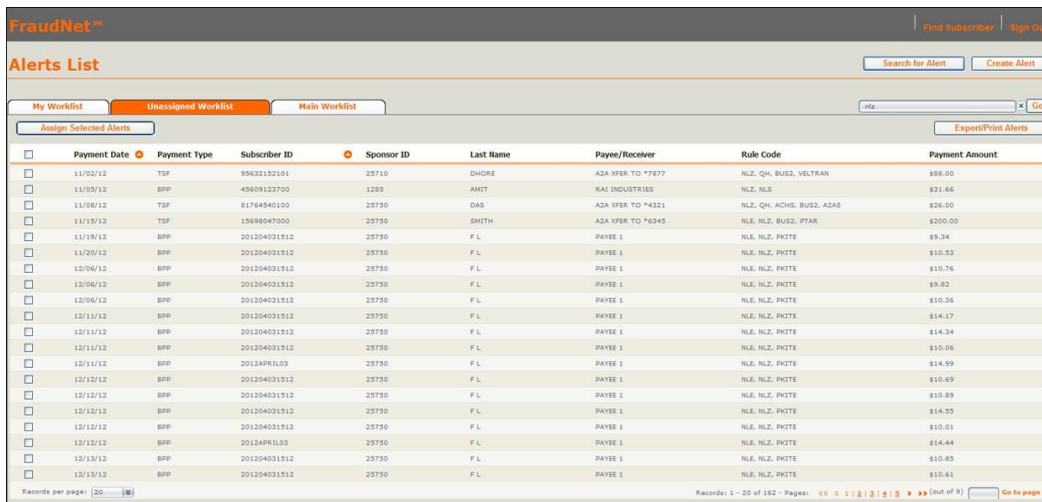
User ID: \*

Password: \*

Use of this system is restricted to authorized users only. Individuals using this computer system may have their activity monitored and recorded. Anyone using this system expressly consents to such monitoring. Unauthorized use will be prosecuted.

\*Required fields **Sign In**

The Alerts List screen will display upon signing in:



The Alerts List screen shows a table of alerts with columns for Payment Date, Payment Type, Subscriber ID, Sponsor ID, Last Name, Payee/Receiver, Rule Code, and Payment Amount. It includes navigation tabs for My Worklist, Unassigned Worklist, and Main Worklist, along with search and export options.

	Payment Date	Payment Type	Subscriber ID	Sponsor ID	Last Name	Payee/Receiver	Rule Code	Payment Amount
<input type="checkbox"/>	11/02/12	TGF	95632152101	25710	CHORE	ADA XFER TO *7877	NLZ, QH, BUS2, VELTRAN	\$88.00
<input type="checkbox"/>	11/05/12	BPP	45609123700	1285	AMIT		NLZ, NLS	\$31.46
<input type="checkbox"/>	11/08/12	TGF	61764940100	25750	DAS	ADA XFER TO *4321	NLZ, QH, ACHG, BUS2, ADAS	\$26.00
<input type="checkbox"/>	11/15/12	TGF	15698047000	25750	SMITH	ADA XFER TO *6345	NLE, NLZ, BUS2, PTAR	\$200.00
<input type="checkbox"/>	11/19/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$9.34
<input type="checkbox"/>	11/20/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.53
<input type="checkbox"/>	12/06/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.76
<input type="checkbox"/>	12/06/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$9.82
<input type="checkbox"/>	12/06/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.36
<input type="checkbox"/>	12/11/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$14.17
<input type="checkbox"/>	12/11/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$14.34
<input type="checkbox"/>	12/11/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.06
<input type="checkbox"/>	12/11/12	BPP	2012APR103	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$14.99
<input type="checkbox"/>	12/12/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.49
<input type="checkbox"/>	12/12/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.89
<input type="checkbox"/>	12/12/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$14.55
<input type="checkbox"/>	12/12/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.01
<input type="checkbox"/>	12/12/12	BPP	2012APR103	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$14.44
<input type="checkbox"/>	12/13/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.85
<input type="checkbox"/>	12/13/12	BPP	201204031512	25750	F L	PAYEE 1	NLE, NLZ, PKITE	\$10.61

Records per page: 20 30 Records: 1 - 20 of 162 - Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 Go to page »

### Assigning Cases

1. From the Alerts List screen, click the **Unassigned Worklist** tab.
2. Determine the number of cases to assign to each fraud specialist and select the cases to assign by selecting the check boxes on the left.

### 3. Select **Assign Selected Alerts**.

Assign Selected Alerts			
<input type="checkbox"/>	Payment Date	Payment Type	Subscriber ID
<input checked="" type="checkbox"/>	11/02/12	TSF	95632152101
<input checked="" type="checkbox"/>	11/05/12	BPP	45609123700
<input checked="" type="checkbox"/>	11/08/12	TSF	81764540100
<input checked="" type="checkbox"/>	11/15/12	TSF	15698047000
<input checked="" type="checkbox"/>	11/19/12	BPP	201204031512
<input checked="" type="checkbox"/>	11/20/12	BPP	201204031512

### 4. Select the agent/specialist to assign the case to:

### Assign Selected Alerts

Update information and click Save to assign the selected alerts.

☒ Assign to Me
   
☐ Assign to Agent

- To assign cases to yourself, select Assign to Me and click **Save**. Your cases will appear in **My Worklist**.
- To assign cases to another user, select Assign to Agent and specify the agent. To see available agents, use the drop-down list. Click **Save** and the cases will then appear only in the selected agent's worklist.
- To assign cases to a business unit (if there are multiple business units), select Assign to Business Unit and specify the business unit. To see available business units, use the drop-down list. Click **Save** and the cases will then appear only in the selected business unit's worklist.

## Accessing Alerts

### 1. Click the **My Worklist** tab in the upper-left corner of the Alerts List page.

Your assigned alerts are displayed.

FraudNet™

Alerts List

Agent: YKGC1007 - MCCABE PAT

My Worklist

Unassigned Worklist

Main Worklist

Assign Selected Alerts

Work All My Alerts

<input type="checkbox"/>	Payment Date	Payment Type	Subscriber ID	Sponsor ID
<input type="checkbox"/>	11/27/12	BPP	22373953600	25710
<input type="checkbox"/>	12/20/12	NDP	26107001500	25710

Records per page: 20



## Note

To change how the alerts are sorted, click on any column header. An arrow inside an orange circle indicates the sort direction. By default, alerts are sorted by Payment Date (earliest payment date first) and then sorted by the Subscriber ID for that date.

- To begin working alerts for the day, click **Work All My Alerts**. This will bring up the My Alerts and Alert Details page. All assigned alerts can be worked from this page

**Alerts List**

Agent: YKGC1007 - MCCABE PAT

My Worklist | Unassigned Worklist | Main Worklist

Assign Selected Alerts | **Work All My Alerts** (indicated by a red arrow)

Payment Date (sorted) | Payment Type | Subscriber ID (sorted) | Sponsor ID

**FraudNet™** Back to Lists | Find Subscriber | Sign Out

**My Alerts** YKGC1007 - MCCABE PAT Alert Count: 2

Payment Date	Payment Type	Subscriber ID	Sponsor ID	Last Name	Payee/Receiver	Rule Code	Payment Amount	Alert Status
11/27/2012	BPP	22373953600	25710	SANCHEZ	AMERICAN EXPRESS	NLS	\$100.00	FollowUp
12/20/2012	NDP	26107001500	25710	ABC	GMAC MORTGAGE	QH, ACHG, PTAR	\$1,100.00	InProcess

**Alert Details** Associated Case | History | Manage Subscriber | Print

Alert Date: 11/23/12 | Alert Status: FollowUp | Alert Type: NegativeLists | Rule Code: NLS

**Subscriber**

Name: OMERLY SANCHEZ  
Address: 5595 PRIVATE ROAD 126  
City: ELIZABETH  
State, ZIP: OH 80107  
Daytime Phone: 678-324-5610  
Evening Phone: 678-324-5610  
Email Address: [TEST@GGG.COM](mailto:TEST@GGG.COM)  
Sponsor ID: 25710  
Subscriber ID: 22373953600  
SSN/TaxID: [888-88-8888](#)  
Universal ID: -  
Birth Date: 01/01/1983  
Enrollment Date: 03/27/10  
Maintenance Date: 11/21/12

**Payment**

Source Account  
Bank Name: LIZ BANK 03  
RT: 061000104  
Account #: [5896589632](#)  
Account Type: DDA

Payment  
Payment Date: 11/27/12  
Payment Type: BPP  
Amount: \$100.00  
Server Tran Time: [2012-11-23-06:13:32.6...](#)  
Payment Schedule: -

Payee  
Name: AMERICAN EXPRESS  
Account #: [372859428498099](#)  
Phone: 800-528-4800  
Address: PO BOX 360001  
City: FORT LAUDERDALE  
State: FL  
ZIP: 33338-0001-01  
Remit Center: 000000122  
Industry Code: 0050  
Payee Modification: None

**IP Geolocation**

IP Address	Carrier	ASN	Country (%)	State (%)	City (%)	Anonymizer Status	Continent
172.24.4.18	-	-	-	-	-	-	-

- Clicking alerts in the top section will populate the Alert Details, which will allow the alert to be worked.



## Searching for an Alert

Specialists can search for alerts by all fields in the following screenshot. There is no timeframe limitation, and both worked and unworked alerts can be found.

## Search for Alert

Type search options and click Search.

### Alert Search Options

Alert Date:\*\*   to  


Alert Status:\*

Alert Type:

Rule Code:   
Separate multiple rule codes with commas.

Agent:

Business Unit:

Decision Date:\*\*  

### Subscriber Search Options

Subscriber ID:


Sponsor ID:

Subscriber Last Name:

### Payment Search Options

Payment Type:

Payment Amount:  to

Payment Date:\*\*  

Payee/Receiver Name:

\* Alert Status is required.  
\*\* Alert Date, Decision Date or Payment Date is required.

## Accessing Subscriber Transaction History

From the Alert Details page, the subscriber transaction history may be accessed by clicking the **Subscriber Transactions** link in the upper-right of the screen.

Transaction history can be used to:

- Link non-alerted transactions to the alert being worked.
- Update the negative files with historical fraud data (e.g., payee ZIP codes and payee account numbers).
- View a specific transaction in PartnerCare by clicking the linked timestamp.
- Sort and group payments in chronological order by timestamp for analysis of consumer behavior.

## Linking Non-Alerted Transactions

When confirmed fraud is identified, choose any associated transactions from the transaction history by selecting the check boxes to the left of the transactions.

Fraudulent payments that did not alert that could also be stopped or otherwise mitigated due to the payment that did alert ("parent" payment/alert) should be linked. Transactions will not be able to be selected if they are already linked to an alert.

### Important

It is critical that specialists mark fraudulent transactions that did not alert. Transactions that were not detected may still be able to be stopped through PartnerCare or by placing a manual stop payment on a draft check.

Subscriber Transactions											
Select subscriber transactions and click the Save button to link selected transactions to the alert.											
Linked to Alert	Server Tran Time	Payee / Receiver Name	Payee/Receiver Account #	Payee Zip	Amount	Payment Date	Status	Source RT	Source Account #	Assoc... Case	Negative Lists
<input checked="" type="checkbox"/>	2013-01-02-22:41.17.23...	ONLINE BILL PMT	FEE	30092-1...	\$0.20	01/01/13	Processed	0611012...	98745632		
<input checked="" type="checkbox"/>	2012-12-05-01:18.53.27...	A2A XFER TO *9632	TRANSFER PYMT FEE	30092-1...	\$10.00	12/12/12	Pending	0611012...	3653653653		
<input type="checkbox"/>	2012-12-05-01:18.51.79...	A2A XFER TO *9632	A2A DIRECT PAYEE	-	\$1.36	12/12/12	Pending	0611012...	3653653653		Negative List Updates
<input type="checkbox"/>	2012-12-04-01:22.09.53...	East Bay Mud	33698574	94649-0...	\$5.00	12/11/12	Pending	0611012...	3653653653		Negative List Updates
<input type="checkbox"/>	2012-12-03-22:48.02.27...	ONLINE BILL PMT	FEE	30092-1...	\$1.20	12/01/12	Processed	0611012...	98745632		
<input type="checkbox"/>	2012-12-03-22:48.02.27...	ONLINE BILL PMT	FEE	30092-1...	\$5.55	12/01/12	Processed	0611012...	98745632		
<input type="checkbox"/>	2012-12-03-05:11.28.71...	Geico Insurance	EXPEDITED PYMT FEE	30092-1...	\$10.00	12/03/12	Processed	0611012...	5896325874		
<input type="checkbox"/>	2012-12-03-05:11.28.61...	Geico Insurance	6666666666	20810-0...	\$5.10	12/03/12	Processed	0611012...	5896325874		Negative List Updates
<input type="checkbox"/>	2012-12-03-01:20.48.80...	A2A XFER TO *3653	TRANSFER PYMT FEE	30092-1...	\$10.00	12/10/12	Pending	0610001...	123456789		
<input type="checkbox"/>	2012-12-03-01:20.48.40...	A2A XFER TO *3653	A2A DIRECT PAYEE	-	\$3.30	12/10/12	Pending	0610001...	123456789		Negative List Updates
Records: 1 - 200 of 1596 - Pages: << < 1   2   3   4   5 > >> (out of 8) <input type="text"/> Go to page >>											
										<input type="button" value="Save"/>	<input type="button" value="Close"/>

Click **Save**. The transactions are now linked to this case and can be used in reporting and statistical analysis.

## Updating Negative Lists Through the Transaction History

To update the FraudNet negative lists from the Subscriber Transaction History window, click on **Negative List Updates**:

Negative List Updates	
Select values and click Save to update the corresponding negative lists.	
Negative List Updates:	<input type="checkbox"/> Source Bank Account # - 61101210 - 3653653653
Case Notes:	<div>Enter case notes here.</div> <div>2000 characters remaining</div>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

## Viewing a Transaction in PartnerCare

To view a specific transaction in PartnerCare, click the transaction's timestamp link in the Subscriber Transactions window. This timestamp is the actual time that the payment was submitted by the subscriber.

<input type="checkbox"/>	<a href="#">2012-12-05-01:18.51.79...</a>	A2A XFER TO *9632	A2A DIRECT PAYEE	-	\$1.36	12/12/12	Pending	0611012...	3653653653	Negative List Updates
--------------------------	---	-------------------	------------------	---	--------	----------	---------	------------	------------	-----------------------

In PartnerCare, you can view the transaction information in greater detail:

[Back](#) [Next](#) | [Work List](#) | [Search](#) | [Admin](#) | [PartnerCare 2](#) [Help](#) | [Sign Out](#)

**Subscriber Snapshot** ?

**Name:** KATERYNA ZHURAVSKA  
**Address:** 3636 MOUNTAIN RD  
Harrison, AR 72601  
**Phone:** 678-324-5610  
Daytime 678-324-5610 Evening  
**E-mail:** test@ggg.com  
**SSN/Tax ID:** 888888888  
**Subscriber ID:** 22373953600  
**Subscriber Account Status:** Frozen  
**Descriptor:**  
**Product:** INTEROPERABLE  
**Processing Method:** Due date  
**Security Answer:**  
**Sponsor ID:** 25710  
**Sponsor Name:** WP 40 REGRESSION ...  
**Enroll Date:** 03/27/10

[Quick Links](#)  
[Password Maintenance](#)  
[Launch Compass](#)

**KATERYNA ZHURAVSKA** | [Account Overview](#) | [Subscriber Profile](#) ? | [Historical Log](#) ?

**Transfer** [Cancel Transfer](#) [Open Case](#) ?

From/To	Routing #	Account #	Type	Debit Process	Credit Process	Transfer Amount	Status	Info...
From	061101210	3653653653	Money M...	12/24/12		1.36	Pending	
To	061000104	5896589632			12/24/12			

**Transfer Details** ?

From/To	Bank Name	Account #	Trace #	Transmit Date	Request Date	Fee Amount	
From	santosh	3653653653		12/24/12	12/12/12	10.00	<a href="#">Recurring Model</a>
To	Jai Ho	5896589632					

**Exception(s)** ?

No exceptions occurred.

## Updating a Case

Update a case for confirmed fraud (see below) or to release a transaction (see “Updating a Case to Release a Transaction” on page 25).

## Updating a Case for Confirmed Fraud

1. For alerted payments that were confirmed as fraudulent, click **Reject** on the right side of the Alert Details page to open the Reject Payment window.

**Reject Payment**

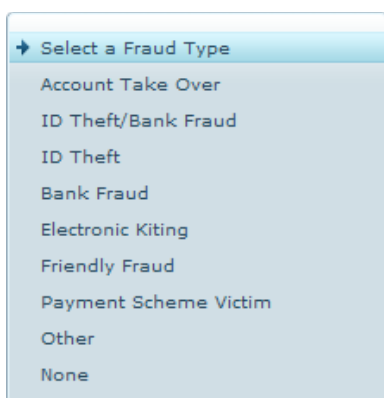
Update information and click Save to reject the payment and take ownership of this alert.

**Payment Action:** Reject  
**Alert Status:** Fraud  
**Fraud Type:** Select a Fraud Type  
**Subscriber Status:** Select a Subscriber Status  
**Negative List Updates:**
☐ Email Address - CCR18@FRAUD.COM  
☐ SSN/Tax ID - 741-32-1654  
☐ Source Bank Account # - 061104107 - 65465465444  
☐ Payee Account # - 678375333  
☐ Payee ZIP Code - 45274-2596-96  
☐ IP Address - 120.43.21.32

**Case Notes:**  
 Enter case notes here.  
 2000 characters remaining

\* Required fields [Save](#) [Cancel](#)

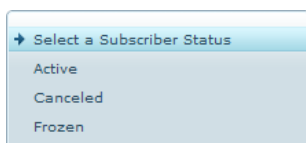
2. In Fraud Type, select the fraud type:



A dropdown menu titled "Select a Fraud Type" with the following options: Account Take Over, ID Theft/Bank Fraud, ID Theft, Bank Fraud, Electronic Kiting, Friendly Fraud, Payment Scheme Victim, Other, and None.

For more information about fraud types, see "Terminology" on page 1.

3. Select the Subscriber Status (Canceled or Frozen):



A dropdown menu titled "Select a Subscriber Status" with the following options: Active, Canceled, and Frozen.

- A Frozen status restricts the subscriber from accessing bill pay.
- A Canceled status also restricts access, but also prevents future bill pay registration across **all** clients using bill pay through Fiserv. As such, this should only be used in cases where there has been subscriber-confirmed identity theft, and they have no intent of using bill pay in the future.

4. Update the appropriate negative lists. However, exercise caution when updating the negative lists. Do not update the negative lists with any of the following:

Negative List	Do not update with...
Email address	noone@noone.com Used as a default email address in the payment system.
Social Security number	any default SSN (e.g., 000-00-0000, 111-11-1111, 777-77-7777, etc.)
Source bank account	a common source bank account (settlement account)
Payee account number	PAYMENT Used as a default value for the payee account number in the payment system.
Payee ZIP Code	A PO Box address or payment address linked to common payees. Typically, these include all addresses that are associated with managed payments, and these will not be able to be selected.
IP Address	Avoid adding any publicly accessible or private IPs. See Geolocation Detection Rules for additional information.

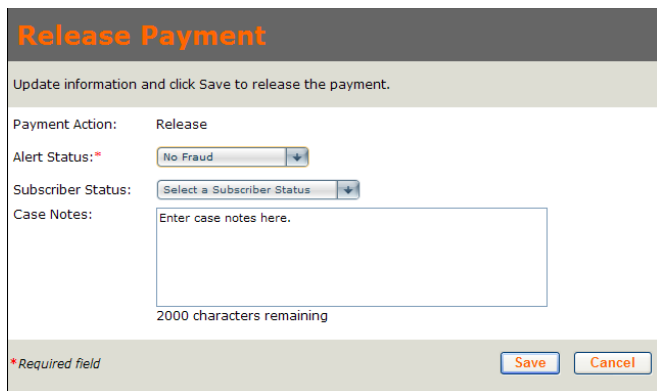
5. Enter Case Notes and click **Save**.

Case notes can be entered manually into the FraudNet Alert Manager and are appended to the PartnerCare case history. This allows for transparency between fraud operations and customer care teams. Fraud specialists should leave notes that are as detailed as possible. Notes should be assumed to be confidential and not to be read or explained to subscribers. Fiserv associates should explicitly note this if sensitive information on the investigation is contained in the note.

## Updating a Case to Release a Transaction

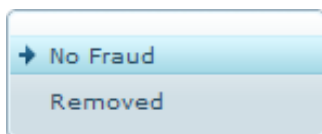
Use the following process when a payment is valid and should be released.

1. Click **Release** on the right side of the Alert Details section of the page to open the Release Payment window.



The screenshot shows the 'Release Payment' window. At the top, it says 'Update information and click Save to release the payment.' Below this, there are four fields: 'Payment Action:' with a value of 'Release'; 'Alert Status: \*' with a dropdown menu showing 'No Fraud'; 'Subscriber Status:' with a dropdown menu showing 'Select a Subscriber Status'; and 'Case Notes:' with a text area containing the placeholder 'Enter case notes here.' and a '2000 characters remaining' indicator. At the bottom left, there is a red asterisk and the text '\* Required field'. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

2. Select "No Fraud" under Alert Status:



The screenshot shows a dropdown menu for 'Alert Status'. The top option is 'No Fraud' with a blue arrow icon. The bottom option is 'Removed'.

### Note

The Removed status is only used when there is a system malfunction and alerts must be removed from the alert queue.

3. If the profile is not already active, select Active under Subscriber Status:



The screenshot shows a dropdown menu for 'Subscriber Status'. The top option is 'Select a Subscriber Status' with a blue arrow icon. The bottom option is 'Active'.

### Note

If the profile is already active, and Active is chosen in this step, an error message may be generated.

4. Case notes should indicate how payment validity was confirmed. Do not leave this field blank or put only "no fraud."
5. Click **Save**.

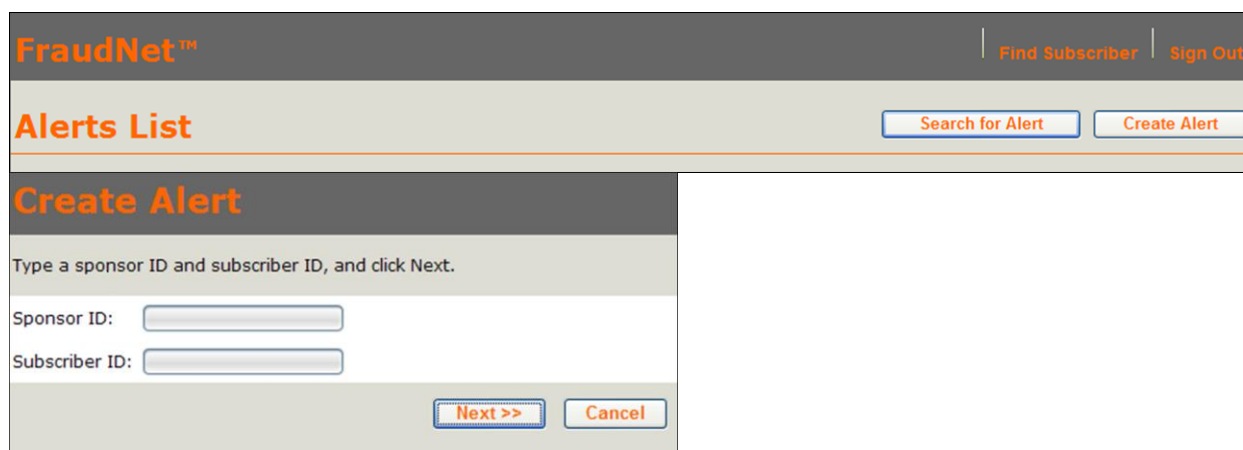
## Manual Alerts

### Creating Manual Alerts

#### Important

A manual alert should be created when a fraudulent payment notification/case is received from an external source and was not detected by FraudNet. Manual alerts are critical to statistical analysis to improve rules and the underlying model.

1. Click **Create Alert** on the upper-right corner of the Alerts List screen to display the Create Alert window.



The screenshot shows the FraudNet interface. At the top, there's a header with the FraudNet logo and links for 'Find Subscriber' and 'Sign Out'. Below this is a section titled 'Alerts List' with two buttons: 'Search for Alert' and 'Create Alert'. The 'Create Alert' button is highlighted, and a modal window titled 'Create Alert' is open in front of it. This modal window contains the instruction 'Type a sponsor ID and subscriber ID, and click Next.' followed by two input fields: 'Sponsor ID:' and 'Subscriber ID:'. At the bottom of the modal are two buttons: 'Next >>' and 'Cancel'.

2. Specify the sponsor ID and the subscriber ID to be associated with the alert and click **Next**.
3. Assign the case as described in “Assigning Cases” on page 18.

### Working a Manual Alert

After creating an alert and assigning it to an investigator, the investigator/specialist should perform all basic investigative functions:

- Perform link analysis on all applicable data.
- Secure all linked accounts.
- Update negative lists with fraudulent transaction information where applicable.
- Link fraudulent transactions in the subscriber's transaction history to the newly created manual alert. For more information, see “Accessing Subscriber Transaction History” on page 21.

### Marking an Alert for Follow Up

When a case is under investigation and is pending either client, subscriber, or biller follow up to the fraud specialist, the alert should be placed in Follow Up status.

1. Click **Follow Up** on the right side of the Alert Details section of the page to display the following window.

### Mark Alert for Follow Up

Update information and click Save to mark alert for follow up.

Alert Status: Follow Up

Subscriber Status:

Case Notes:

2000 characters remaining

- Specify the subscriber status and add case notes.
- Click **Save**.

The case now appears in your queue with the Alert Status of FollowUp.

Payment Date	Payment Type	Subscriber ID	Sponsor ID	Last Name	Payee/Receiver	Rule Code	Payment Amount	Alert Status
11/27/2012	BPP	22373953600	25710	SANCHEZ	AMERICAN EXP...	NLS	\$100.00	FollowUp

## Viewing the Associated Case

To view the details of a case, click on Associated Case on the Alert Details page. This will open the Subscriber Snapshot and Case Details screen from PartnerCare. Clicking Manage Subscriber will also link to the PartnerCare view of the subscriber and payment. For details about navigating PartnerCare, contact your account representative at Fiserv.

### Subscriber Snapshot

Name: HOWARD WOLOWITZ

Address: 5000 BIG BANG THEORY  
DULUTH, GA 30032

Phone: 404-474-6655  
Evening  
cor18@fraud.com

E-mail: 741321654

SSN/Tax ID: 741321654

Subscriber ID: 74132165400

Account Status: Frozen

Descriptor: \*FRAUD\*

Product: INTEROPERABLE

Processing Method: Due date

Security Question: What is your moth...

Security Answer: tester

Sponsor ID: 25750

Sponsor Name: YP 411 REGRESSION...

Enroll Date: 01/04/13

Quick Links  
Password Maintenance  
Launch Compass

### HOWARD WOLOWITZ

Account Overview | Subscriber Profile | Historical Log

**Be sure to click a button to close, save, or route this case to keep any changes you make.**

#### Case Details # 20077029

Opened by: FRAUD ENGINE | Last Updated by: FRAUD ENGINE | Assigned to: Unassigned

Reason Category: 250-Risk Manag... | Priority: Normal | Status: Open

Case Age: 4 business days | Case Open Date: 01/09/13

Subscriber Provided: Alternate Contact Number: | Account Holder Name: | Payee Contact Name: | Payee Contact Phone: |

Sponsor Follow Up: | Sponsor Reg E: Yes No | CheckFree Reg E: No

#### Case Interaction

Notes | Correspondence

Date	Representative	Notes
1/9/2013 10:06:34 AM	FRAUD ENGINE	1/9/2013 10:06:34 AM FRAUD ENGINE This transaction is currently under review for possible fraudulent activity. Please reference your sponsor information tab for customer referral information. This notice does not mean fraud has taken place.





## Using Link Analysis Functions

FraudNet allows specialists to perform quick link analysis on applicable variables within the FraudNet Alert Manager. The following variables within Alert Details allow for link analysis on all the investigator's bill payment customers:

- Social Security numbers
- Email addresses
- Payee account numbers
- Bank accounts
- Payee ZIP Code (unmanaged payees only)

To run a link analysis, click on any of the data variables listed above within Alert Details. For example, if you click on the payee account number 1234576756 and there are no other subscribers using the same account number in their payee profiles, the following screen appears:

**Alert Link Analysis**

Subscribers associated with source account number:5896589632

Subscriber ID	Sponsor ID	Status	FraudNet Sponsor
No subscriber link analysis results found.			

Close

When there are links to other subscriber profiles, the relevant subscriber ID will be displayed.

**Alert Link Analysis**

Subscribers associated with SSN/Tax ID:261-07-0015

Subscriber ID	Sponsor ID	Status	FraudNet Sponsor
<a href="#">26107001500</a>	25725	Active	Yes
<a href="#">26107001500</a>	25750	Active	Yes
<a href="#">26107001501</a>	25710	Active	Yes
<a href="#">26107001501</a>	25725	Active	Yes
<a href="#">26107001501</a>	25750	Active	Yes
<a href="#">26107001502</a>	25710	Active	Yes
<a href="#">26107001502</a>	25725	Verification	Yes
<a href="#">26107001502</a>	25750	Active	Yes
<a href="#">26107001503</a>	25710	Active	Yes
<a href="#">26107001503</a>	25725	Verification	Yes

Close

If the links that are returned are confirmed as fraudulent accounts and a Manual Alert is necessary, click **Create Alert**. Refer to “Creating Manual Alerts” on page 26 for additional detail.

Alert Link Analysis				
Subscribers associated with SSN/Tax ID:261-07-0015				
Subscriber ID	Sponsor ID	Status	FraudNet Sponsor	
26107001500	25725	Active	Yes	Create Alert
26107001500	25750	Active	Yes	Create Alert
26107001501	25710	Active	Yes	Create Alert

After you click **Create Alert**, a window will appear to validate that the correct subscriber information is being used to create the alert.

### Create Alert

Confirm information and click Create.

Sponsor ID: 25725

Subscriber ID: 26107001500

Subscriber Name: ABC HCYDS

Click **Create** to confirm that the information is correct. Follow the instructions in “Working a Manual Alert” on page 26.

## Working a Popmoney Confirmed Fraud

When dealing with fraudulent Popmoney transactions, investigators/specialists must take actions in both the FraudNet Alert Manager and Compass (see “Compass Restricted Hold / Suspension Procedures” below).

### FraudNet

Within FraudNet, when investigators/specialists click the **Reject** button in the My Alerts window, they are prompted to:

- Specify the Alert Status (Fraud, Customer Error, or Unconfirmed).
- Select a Fraud Type (Account Takeover, ID Theft/Bank Fraud, ID Theft, Bank Fraud, Electronic Kiting, Friendly Fraud, or Payment Scheme Victim).
- Select the Subscriber Status (Canceled or Frozen).
- Update FraudNet Negative Files (Email, SSN/Tax ID (only if applicable), Receiver Account, and/or Sender Account).
- Enter Case Notes (such as Fraud – Reject Payment).

## Compass Restricted Hold / Suspension Procedures

When fraud is detected on a Popmoney transaction via the FraudNet detection system, the fraud investigator/specialist must take the appropriate actions in Compass when the payment is rejected in FraudNet.

### Suspending an Account in Compass

To suspend an account based on FraudNet alert research:

1. From the Risk Management screen, go to Suspension Management and click **Restricted Hold / Suspend** next to an account that you want to suspend.

The note box opens automatically; select the reason from the drop-down list.

#### Confirmed Fraud

- Type in note: "FraudNet Alert – Confirmed Fraud."
- Select reason from drop-down list: "Requested by client – confirmed fraud."

#### Suspicious Activity

- Type in note: "FraudNet Alert – Suspicious activity."
- Select reason from drop-down list: "Linked to Discrepant Activity."

2. Click **Apply Action** and repeat for all accounts you want to suspend.

### Unsuspending an Account in Compass

To unsuspend a profile:

1. From the Risk Management screen, go to Suspension Management and click **Unsuspend** next to an account that you want to unsuspend.
2. From the drop-down list, select the reason "Issue Satisfactorily Resolved" and insert notes.
3. Click **Apply Action** and repeat for all accounts you want to unsuspend.

## Working a Suspicious Transaction Alert

This section contains the process flow for working a suspicious transaction alert in FraudNet.

