Consumer related alerts and messages

Consumer related alerts allow subscribers to identify any consumer credit file that contains personal statements from the consumer pertaining to suspicious activity, potential fraud, or known fraudulent activity. In addition, subscribers are able to identify synthetic identities as well as verify consumer identities or identity elements for compliance with Red Flags and Know-Your-Customer (KYC) regulations. There are eight (8) alerts in this section as described below.

Table I: Consumer related alerts

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
9003	Consumer Statement On File Relates To True Name Or Credit Fraud	The consumer has placed a statement on his/her credit file indicating the potential or presence of identity theft, identity fraud and/or credit fraud.	• System detected a consumer statement on the TransUnion credit file. • Consumer wants to notify companies of important information before further processing transactions. • Potential of compromised or misused identity being used to perpetrate fraud. **Note** Any consumer can place a consumer statement on their credit file. The content of the statement is not returned in this solution due to FCRA requirements.	• Obtain and review content from the consumer statement found at the end of the TransUnion Credit Report for details pertaining to potential fraud and/or identify theft. • If provided, contact consumer at the contact information listed in the consumer statement before proceeding with the transaction.	Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
9004	Active Duty Alert On File	The consumer has placed a statement on his/her credit file indicating that he/she is on active military duty leave.	• System detected an active duty military leave statement on TransUnion's credit file. • Consumer wants to notify companies of his/her active duty military status. • Potential of compromised or misused identity being used to perpetrate fraud. • Consumer may have forgotten to remove the alert upon returning from military duty.	• Contact consumer to verify he/she is the individual conducting the transaction.	Low/ Medium
9005	Initial Fraud Alert On File	The consumer has placed a statement on his/her credit file indicating that he/she might be a victim of identity theft and/or fraud.	• System detected an initial fraud alert on TransUnion's credit file. • Consumer wants to notify companies of potential identify theft or fraud. • Potential of compromised or misused identity being used to perpetrate fraud.	• Contact consumer to verify he/she is the individual conducting the transaction.	Low/ Medium
9006	Extended Fraud Alert On File	The consumer has placed a statement on his/her credit file indicating that he/she has submitted an ID Theft Report and is a reported victim of true name or credit fraud.	• System detected an extended fraud alert on TransUnion's credit file. • This consumer has been reported as a victim of fraud and has filed an ID theft report. • Indicates compromised or misused identity being used to perpetrate fraud.	• Contact consumer to verify he/she is the individual conducting the transaction.	High
9011	Potential Synthetic Identity[1]	The input consumer identity has unknown combinations of real and/or fictitious identity elements as well as	• System detected FCRA and GLBA attribute anomalies and/or discrepancies between input provided and known, established identities within our data network.	• Require consumer to provide documentary proof of his/her identity.	High

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
		other elements typical of synthetic identities.		• Require consumer to pass additional verification and/or authorization procedures.	
9014	New or Recent Identity In Network - Created Within Last two (2) Days	The input consumer identity was recently or added to the TransUnion identity network within the referenced time requirement. Days are configurable. Best industry practice for days = 2.	• System detected new identity in TransUnion network within the referenced creation timeframe.	• Require consumer to pass additional verification and/or authorization procedures.	Medium/ High
9016	Input Consumer Identity Elements - Not Verified	The input consumer identity or identity elements were not verifiable against known identities in the TransUnion data network.	• System detected unverifiable identity elements for the input consumer identity.	• Require consumer to pass additional verification and/or authorization procedures.	Medium/ High
9017	Input Consumer Identity Elements - Verified	The input consumer identity or identity elements were verifiable against known identities in the TransUnion data network.	• System's identity matching threshold was sufficient to consider the input identity or identity elements as verified against TransUnion's data network.	• Follow your company's procedures for verified identities. • May require additional documentary proof of identity.	Low

[1]This alert requires FCRA permissible purpose to be delivered to subscribers. Therefore, these alerts are only returned when this service is provided as an add-on to an FCRA solution, such as the Credit Report (service code: 07000) or Model Report (service code: 08000).

Social Security number (SSN) related alerts and messages

Social Security number (SSN) related alerts and messages available in the IDVision Alerts/Search solutions notify subscribers of any suspicious, high-risk, or known fraudulent SSNs. SSN Year of Issuance informational messages are also provided for SSNs issued prior to activation of SSN Randomization by the Social Security Administration in June of 2011. Unusual SSN usage alerts are also provided to notify subscribers of SSNs that belong to deceased persons or minor, are used by multiple consumers, and/or have been used too frequently on recent inquiries. There are twenty-two (22) Social Security number related alerts and messages are available in this service as shown below.

Table II: Social Security number related alerts and messages

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
3001	SSN Reported As Suspicious	The input or file SSN has been deemed as suspicious due to use in suspected or known fraud or belonging to a minor.	• Input or file SSN matched an SSN on the suspicious ID element database. • Applicant might be using a compromised or misused SSN to perpetrate fraud. • Consumer might be a victim of someone misusing his/her SSN. • Consumer might be misusing a SSN to create a new identity or to obtain credit under a different consumer's identity information.	• Verify accuracy of input SSN. • Verify SSN through documentary procedures to ensure that it belongs to the applicant. • Contact consumer to verify he/she is the person conducting the transaction.	Medium
3003	SSN Reported Misused And Requires Further Investigation	The input or file SSN has been reported as used to attempt fraud or manipulate an identity.	• Input or file SSN matched an SSN on the Misused ID element database. • Same as items 2 through 4 for code 3001 above.	• Same as code 3001 above.	Low/ Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
3004	Input/File *SSN* Belongs To A Minor	The input or file SSN belongs to a consumer under the age of sixteen (16) years old.	• Input/file SSN matched an SSN on a TransUnion database which has been identified as belonging to a person under the age of sixteen (16) years old. • Same as items 2 through 4 for code 3001 above.	• Same as code 3001 above.	High
3005	Input *SSN* Associated With Multiple Consumers As Primary SSN	The input SSN is being used by more than one (1) consumer as the ***primary*** SSN on consumer files. **Note** Best practice setting for multiple consumers is “3”. Number of consumers is an optional setting from 3 to 99.	• Input SSN matched an SSN on the Misused ID element database. • Same as items 2 through 4 for code 3001 above.	• Same as code 3001 above.	Medium
3006	Input *SSN* Associated With Multiple Consumers	The input SSN is being used by more than three (3) people on consumer files. **Note** Best practice setting for multiple consumers is “3”. Number of consumers is an optional setting from 3 to 99.	• Input SSN matched an SSN on the Misused ID element database. • Same as items 2 through 4 for code 3001 above.	• Same as code 3001 above.	Low/ Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
3007	Multiple SSNs On Consumer File	The input consumer has at least three (3) significantly different SSNs on his/her consumer file.	• System detected three (3) or more SSNs on the input consumer's TransUnion's credit file. • Same as items 2 through 4 for code 3001 above.	• Same as code 3001 above.	Low/ Medium
3008	Input/File SSN Involved In Burst Velocity Usage In Multiple Consumer Files	The input or file SSN has a sudden volume increase usage on multiple consumer files within a thirty (30) day period.	• System detected many different consumer files using the same input or file SSN on within a thirty-day period.	• Same as code 3001 above.	Medium/ High
3010	Input SSN Is Invalid - Potential ITIN	The input SSN has been identified as matching the format of an Individual Taxpayer Identification Number (ITIN).	• System identified the input provided SSN meets the format of an ITIN.	• Same as code 3001 above.	Medium
3012	Input SSN Is Invalid - Format	The input SSN has been identified as NOT matching valid formats, structure or characters of SSNs issued by the Social Security Administration (SSA).	• System detected the input provided SSN has an invalid format.	• Same as code 3001 above.	Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
3501	SSN Reported Used In True Name Fraud Or Credit Fraud	The input or file SSN has been reported as used in connection with known fraudulent applications or other transactions.	• Input or file SSN matched an SSN on the known-fraudulent ID element database. • Applicant may be reusing information used in a previous fraudulent transaction. • Same as items 2 through 4 for code 3001 above.	• Same as code 3001 above.	High
4001	SSN Is Reported Deceased	The SSN has been linked to a reported deceased person by institutions, relatives or other agents.	• System detection of deceased indicator on TransUnion's credit file. • The consumer has been reported as deceased by one or more reporting agents. • SSN may be compromised and/or being used to commit fraud. • Potential of compromised or misused identity being used to perpetrate fraud.	• Verify accuracy of input SSN and other identity data. • Require consumer to provide documentary proof of valid and issued SSN. • Conduct proper due diligence based on your company's fraud policies.	High
4501	SSN Likely Not Issued Prior To June 2011	TransUnion is unable to determine if the SSN has been issued by the Social Security Administration (SSA).	• System unable to find SSN on SSA's historical year-of-issuance database. • SSN may or may not have been issued under SSN Randomization – unable to determine. • Applicant may be using a valid SSN. Due to SSN Randomization by the SSA, the SSN cannot be confirmed as being issued to a consumer.	• Same as code 4001 above. • Determine if input SSN matches the file SSN for the consumer by reviewing TransUnion's ID Mismatch or Identity Verification solutions.	Low

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
4506	Input SSN Is Unverifiable	TransUnion is unable to determine if the SSN has been issued by the Social Security Administration (SSA) nor verified as belonging to the consumer by qualified data providers.	• Transunion is unable to verify SSN has been issued by the SSA nor known as belonging to the input consumer from trusted data furnishers. • Same as items 2 through 4 for code 4501 above.	• Same as code 4001 above.	Medium
5501	SSN Has Been Used XX Times In The Last XX Days On Different Inquiries[1]	The Social Security Number (SSN) has been used an unusual number of times in a given time period. **Note** Best practice settings for number of times and days are “6” and “30”, respectively. Subscribers have an option to select number of inquiries from 1 through 99 as well as days as 30, 60 or 90.	• System has detected subscriber selected SSN thresholds for inquiries and days. • Potential of compromised or misused identity being used to perpetrate fraud.	• Verify accuracy of input SSN and other identity data. • Require consumer to provide documentary proof of valid and issued SSN. • Conduct proper due diligence based on your company’s fraud policies.	High

[1]This alert requires FCRA permissible purpose to be delivered to subscribers. Therefore, these alerts are only returned when this service is provided as an add-on to an FCRA solution, such as the Credit Report (service code: 07000) or Model Report (service code: 08000).

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
5502	SSN Associated With Additional Subject(s) Not Displayed/ Returned[1]	The SSN has been linked to multiple consumers.	• SSN may have been improperly entangled with multiple consumers during joint applications, guardian or survivor benefits, or other situation. • Multiple consumers are using the SSN. • Applicant may be fraudulently using a stolen SSN. • Applicant may be using an SSN that belongs to a spouse, parent, or child.	• Same as code 4001 above.	High
5503	SSN Issued Within the Last X Years; Year Issued: 19XX; State: XX; Est. Age Obtained XX	The SSN has been verified as issued by the Social Security Administration (SSA). Data returned includes issuance year range (2, 5 or 10 years), issuance year, state where SSN was issued and estimated age.	• System detected input SSN on SSA's historical year-of-issuance database. • Estimated Age Obtained is calculated by using Year of Issuance and input/file date of birth. • This message is provided for information purposes. • Absence of alert may indicated SSN issued under SSN Randomization or potential fraud.	• Absence of this message may require documentary proof of SSN issuance. **Note** This message cannot be returned with code 5504. Subscriptions can only be setup to receive either 5503 or 5504, but not both.	Low
5504	SSN Issued: 19XX; State: XX Est. Age Obtained: XX	The SSN was issued by the SSA in the given year, state and age.	• Same as code 5503 above.	• Same as code 5503 above **Note** This message cannot be returned with code 5503. Subscriptions can only be setup to receive either 5503 or 5504, but not both.	Low

[1]This alert requires FCRA permissible purpose to be delivered to subscribers. Therefore, these alerts are only returned when this service is provided as an add-on to an FCRA solution, such as the Credit Report (service code: 07000) or Model Report (service code: 08000).

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
5506	Input SSN Has An Unusual Number (X) of Inquiries In The Last (Y) Days	The Social Security Number (SSN) has been used an unusual number of times in a given time period. **Note :** Best practice settings for unusual number of inquiries and days are “5” and “2”, respectively. Subscribers have an option to select number of inquiries from 1 to 99 as well as days from 1 to 90.	• System has detected subscriber selected SSN thresholds have been surpassed for inquiries and days. • Potential compromised or misused identity or identity element.	• Verify accuracy of input SSN and other identity data. • Require consumer provide proof of valid and issued SSN. • Conduct proper due diligence based on your company’s fraud policies.	High
5507	Input SSN Has An Unusual Number (8) Of Inquiries In The Last (4) Days	Same as alert 5506. However, the best practice thresholds for inquiries and days are different to allow tracking and evaluation of different metrics.	• Same as above.	• Same as above.	High
5508	Input SSN Has An Unusual Number (15) Of Inquiries In The Last (7) Days	Same as alert 5506. However, the best practice thresholds for inquiries and days are different to allow tracking and evaluation of different metrics.	• Same as above.	• Same as above.	High

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
5999	SSN Requires Further Investigation	The SSN may have been involved in potentially risky transactions.	• Input or file SSN matched an SSN that may have been used inappropriately in identity theft. • Applicant might be using a compromised or misused SSN to perpetrate fraud. • Consumer might be a victim of someone misusing his/her SSN. • Consumer might be misusing his/her SSN to create a new identity or to obtain credit under a different consumer's identity information.	• Verify accuracy of input SSN. • Verify SSN through documentary procedures to ensure that it belongs to the applicant. • Contact consumer to verify that he/she is actually conducting the transaction.	Low
6000	SSN Used In Death Benefits Claim	The SSN belongs to a consumer reported as deceased by the SSA. Data returned includes the SSN, date of birth, date of death, name of deceased person, and location where death benefits were paid.	• System detection of deceased person based on input or file SSN. • Surviving spouse/benefactor may be using the SSN of deceased person. • Deceased person's SSN might be improperly entangled with the SSN of the surviving spouse or benefactor. • Potential of compromised or misused SSN being used to perpetrate fraud.	• Same as code 5999 above. • Determine if any other consumers are associated with the SSN (see codes 3005, 3006, 3008 and 5502).	High

Address related alerts and messages

Address related alerts and messages available in the IDVision Alerts/Search services notify subscribers of any suspicious, high-risk, or known fraudulent addresses. Often, there are attempts to use commercial addresses to pose as legitimate residential addresses to take over consumer accounts and commit fraud. This service will identify high-risk commercial addresses as well as addresses that have been reported as used in fraud cases plus. In addition, our address related alerts will notify subscribers of any unusual address usage that is typically fraud related. There are thirty-four (34) address related alerts available in this solution.

Table III: Address related alerts and messages

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
0001	Address Is A Mail Receiving/Forwarding Service	The consumer is using a commercial address to pose as a residential address.	• Input or file address matched an address belonging to a commercial establishment. • Applicant may be in temporary residence in a commercial facility. • Applicant may be an employee at a residential institution. • Consumer might be misusing the address to create a new identity or to commit fraud.	• Verify accuracy of input address. • Verify address through documentary procedures to determine if it belongs to the consumer. • Contact consumer to verify he/she is actually conducting the transaction.	Medium
0002	Address Is A Hotel/Motel or Temporary Residence				Medium
0003	Address Is A Credit Correction Service				Low
0004	Address Is A Camp Site				Low
0005	Address Is A Secretarial Service				Low
0006	Address Is A Check Cashing Service				Low

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
0007	Address Is A Restaurant/Bar/ Nightclub				Low
0008	Address Is A Storage Facility				Low
0009	Address Is An Airport/ Airfield				Low
0010	Address Is A Truck Stop				Low
0500	Address Is Commercial				Medium
0501	Address Is A Correctional Institution				Medium
0502	Address Is A Hospital Or Clinic				Low
0503	Address Is A Nursing Home				Low
1000	Address Is Institutional				Low
1001	Address Is A US Post Office	The consumer is using a commercial address to pose as a residential address.	• Input or file address matched an address belonging to a government building.	• Same as code 0001 above.	Low/ Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
1500	Address Is Governmental	The consumer is using a known-government address to pose as a residential address.	• Applicant might be renting a P.O. Box at the post office. • Applicant may be an employee at a government establishment. • Consumer might be misusing the address to create a new identity or to commit fraud.	• Same as code 0001 above.	Medium
1501	Address Reported As Suspicious	The input or file address has been deemed as suspicious due to use in suspected or known fraud.	• Input or file address matched an address on the suspicious ID element database. • Applicant might be using a compromised or misused address to perpetrate fraud. • Consumer might be a victim of someone misusing his/her address. • Consumer might be misusing his/her address to create a new identity or to obtain credit under a different consumer's identity information.	• Verify accuracy of input address. • Verify address through documentary procedures to ensure that it belongs to the applicant. • Contact consumer to verify he/she is actually conducting the transaction.	Low
1502	Address Is A Multi-Unit Building Reported as Suspicious	The address is an apartment building that couldn't be verified on previous transactions and has been reported as potentially compromised.	• Same as code 1501 above.	• Same as code 1501 above.	Low
1503	Address Reported Misused And	The address has been reported as used to	• Same as code 1501 above.	• Same as code 1501 above.	Low

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
	Requires Further Investigation	attempt fraud or manipulate an identity.			
1504	Address Is A Multi-Unit Building Reported Misused And Requires Further Investigation	The address is an apartment building that couldn't be verified on previous transactions and has been reported as potentially compromised.	• Same as code 1501 above.	• Same as code 1501 above.	Low
2001	Address Reported Used In True Name Fraud Or Credit Fraud	The input or file address has been reported as used in connection with known fraudulent applications or other transactions.	• Input or file address matched an address on the known-fraudulent ID element database. • Applicant may be reusing information used in a previous fraudulent transaction. • Applicant might be using a compromised or misused address to perpetrate fraud. • Consumer might be a victim of someone misusing his/her address. • Consumer might be misusing his/her address to create a new identity or to obtain credit under a different consumer's identity information.	• Same as code 1501 above.	Low/ Medium
2010	More Recent Address Available for Consumer. New Address Reported As	Consumer has a more recent address on file than the address provided with the input data. The more	• System detected a more recent address on the consumer's file. • Consumer may live at multiple addresses such as a	• Verify through documentary procedures that the input address is actually the	Low

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
	<file address> On <first reported date>	recent address is returned as well as the first date reported.	summer/winter home or college facility. • Customer may be using an improper address to commit fraud.	consumer's current address.	
2501	Address Has Been Used XX Times In The Last XX Days On Different Inquiries[1]	The address has been used in an unusual pattern that may indicate potential fraud. **Note** Best practice settings for times address used and days are "6" and "30", respectively. Subscribers have an option to select number of times from 1 to 99 as well as days as 30, 60 or 90.	• Consumer might be applying for new credit with multiple financial companies. • Multiple members of the same household may be applying for credit at the same time. • Applicant might be misusing address to commit fraud. • Consumer may have been a victim of someone trying to take over a credit account.	• Verify accuracy of input address. • Verify address through documentary procedures to ensure that it belongs to the applicant. • Contact consumer to verify he/she is actually conducting the transaction. • Look for discrepancies between Address and SSN velocity messages. Discrepancies could indicate fraud attempts.	Low/ Medium

[1]This alert requires FCRA permissible purpose to be delivered to subscribers. Therefore, these alerts are only returned when this service is provided as an add-on to an FCRA solution, such as the Credit Report (service code: 07000) or Model Report (service code: 08000).

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
2502	Address Has Been Reported More Than Once (Up To 10 PO Boxes Or Unit #s)	More than one data contributor has previously reported the input or file address as suspicious.	• Consumer may have been a victim of an account takeover. • Consumer might be using a compromised or misused address to perpetrate fraud. • Consumer might be misusing his/her address to create a new identity.	• Verify accuracy of input address. • Evaluate in conjunction with other alerts; proceed with suggested actions from other alerts. **Note** This alert may appear in conjunction with other high-risk alerts, and suggests a stronger indication of potential fraud.	Low/ Medium
2503	File Address Tenure Indicative Of Potential Fraud	Consumer has an unusual and potentially fraudulent address history	• Consumers has moved an unusual number of times or additional addresses have been reported for the consumer in an unusual time frame. • Same as items 2 through 4 for code 2001 above.	• Same as code 1501 above.	High

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
2504	Input current *Address* Has An Unusual Number (X) Of Inquiries In The Last (Y) Days	The input address has been used in an unusual pattern that may indicate potential fraud. **Note** Best practice settings for unusual number of inquiries and days are "5" and "2", respectively. Subscribers have an option to select number of inquiries from 1 through 99 as well as days from 1 through 90.	• System has detected subscriber selected address thresholds have been surpassed for inquiries and days. • Potential compromised or misused identity or identity element. • Multiple consumers might be using the same address on different transactions. • Applicant might be misusing this address to commit fraud.	• Verify accuracy of input address and other identity data. • Require consumer provide proof that he/she lives at that input address. • Conduct proper due diligence based on your company's fraud policies. • Determine if discrepancies exists between Address and SSN velocity messages. Discrepancies could indicate fraud attempts.	Medium
2505	Input Current Address Has An Unusual Number (8) Of Inquiries In The Last (4) Days	Same as alert 2504. However, the best practice thresholds for inquiries and days are different to allow tracking and evaluation of different metrics.	• Same as above.	• Same as above.	Medium
2506	Input Current Address Has An Unusual Number (15) Of	Same as alert 2504. However, the best practice thresholds for inquiries and days are	• Same as above.	• Same as above.	Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
	Inquiries In The Last (7) Days	different to allow tracking and evaluation of different metrics.			
2507	Input Current Address Tenure Is (XXX) Month(s)	The input consumer has lived at the current address the specified number of months.	• Input current address match the address on file for the consumer. The address first reported date and transaction date was used to calculate the address tenure.	• This is an informational message to help determine how long a consumer has lived at the input address. Usage or suggested actions should be based on your company procedures.	Low
2999	Address Is A Multi-Unit Building	The address is a building with multiple dwellings such as apartments or office building.	• Input or file address matched an address listed as an apartment building or other multi-unit building. • Same as code 2502 above.	• Verify accuracy of input address. • Verify address through documentary procedures to ensure that it belongs to the applicant. • Contact consumer to verify he/she is actually conducting the transaction.	Low
3000	Address Requires Further Investigation	The input or file address may have been involved in potentially risky transactions.	• Input or file address matched an address that may have been used inappropriately in identity theft. • Same as code 2502 above.	• Same as code 2502 above.	Low

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
9001	Address, SSN And/Or Telephone Number Reported Together In Suspected Misuse	At least two of the input elements (address, SSN, and/or telephone number) were used together in suspected or known fraud.	• Same as code 2502 above.	• Same as code 2502 above.	Low/ Medium
9002	Address, SSN, Or Telephone Number Reported By More Than One Source	More than one data contributor has reported at least one of the input or file ID elements as suspicious.	• Consumer may have been a victim of an account takeover. • Consumer might be using a compromised or misused address, SSN or phone number. • Consumer might be misusing his/her address to create a new identity or commit fraud.	• Same as code 2502 above.	Low/ Medium

Telephone number related alerts and messages

Telephone Number related alerts and messages available in the IDVision Alerts/Search services notify subscribers of any suspicious, high-risk, or known fraudulent telephone numbers. Often the type of telephone number used in a transaction can help identify potential fraud. Phone numbers belonging to commercial and institutional properties can represent higher risks than consumer phone numbers. In addition, past trends indicate that cellular phone, public/pay phone, or answering service can have a high-risk of fraud. In addition, this service now offers alerts that identify unusual phone usage to assist in detecting fraud. Thirteen (13) telephone number related alerts and messages are available in this service.

Table IV: Telephone number related alerts and messages

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
6001	Telephone Number Is An Answering Service	The telephone number belongs to a commercial answering service.	• Input or file phone number matched the profile of a high-risk telephone number. • Consumer is using a public phone or "pay as you go" phone as a residential phone. • Consumer might be misusing the telephone number to create a new identity or commit fraud.	• Verify accuracy of input phone number. • Verify phone number through documentary procedures to ensure that it belongs to the consumer. • Contact consumer to verify he/she is actually conducting the transaction. • Review your company's policy on accepting non-residential or suspicious telephone numbers	Low
6002	Telephone Number Is A Cellular Telephone	The telephone number belongs to a mobile phone system.			Low
6003	Telephone Number Is A Public/Pay Phone	The telephone number belongs to a land-based, coin/credit card operated public phone.			Low/ Medium
6021	Input Telephone Number Has An Unusual Number (5) Of Inquiries In The Last (2) Days	The input telephone number has been used in an unusual pattern that may indicate potential fraud.			Low/ Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
		Note Best practice settings for unusual number of inquiries and days are “5” and “2”, respectively. Subscribers have an option to select number of inquiries from 1 through 99 as well as days from 1 through 90.		on applications/ transactions.	
6022	Input Telephone Number Has An Unusual Number (8) Of Inquiries In The Last (4) Days	Same as alert 6021. However, the best practice thresholds for inquiries and days are different to allow tracking and evaluation of different metrics.			Low/ Medium
6023	Input Telephone Number Has An Unusual Number (15) Of Inquiries In The Last (7) Days	Same as alert 6021. However, the best practice thresholds for inquiries and days are different to allow tracking and evaluation of different metrics.			Low/ Medium
6500	Telephone Number is Commercial	The telephone number matched a list of various			Low/ Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
7000	Telephone Number Is Institutional	non-residential telephone numbers.			Low
7500	Telephone Number Is Governmental				Low
7501	Telephone Number Reported As Suspicious	The phone number couldn't be verified on previous transactions and has been reported as potentially compromised.	• Input or file phone number matched same on TransUnion's suspicious telephone number database. • Applicant might be using a compromised or misused phone number to perpetrate fraud. • Consumer might be a victim of someone misusing his/her phone number. • Consumer might be misusing the phone number to create a new identity or to obtain credit under a different identity.	• Same as code 6001 above	Low/ Medium
7503	Telephone Number Reported Misused And Requires Further Investigation	The input or file phone number has been reported as used to attempt fraud or manipulate an identity.	• Input or file phone number matched the same on the suspicious ID element database. • Applicant might be using a compromised or misused phone number to perpetrate fraud. • Consumer might be a victim of someone misusing the phone number. • Consumer might be misusing the phone number to create a new	• Same as code 6001 above	Low/ Medium

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
			identity or to obtain credit under a different identity.		
8001	Telephone Number Reported Used In True Name Fraud Or Credit Fraud	The input or file phone number has been reported as used in connection with known fraudulent applications or other transactions.	• Input or file phone number matched the same on the known-fraudulent ID element database. • Applicant may be reusing information used in a previous fraudulent transaction. • Same as items 2 through 4 for code 6001 above.	• Same as code 6001 above	Medium/ High
9000	Telephone Number Requires Further Investigation	The input or file phone number may have been involved in potentially risky transactions.	• Input or file phone number may have been used inappropriately in identity theft. • Applicant might be using a compromised or misused phone number to perpetrate fraud. • Consumer might be misusing the phone number to create a new identity or to obtain credit under a different identity.	• Same as code 6001 above	Low

Product status-related alerts

Product Status-related alerts notify subscribers of problems or the lack thereof, related to the status of their IDVision Alerts/Search transaction results. Four (4) status related messages are available in this service as shown below.

Table V: Product status related alerts

Code	Text description	What does it mean?	Why was it generated?	Suggested actions	Risk level
9996	IDVision Alerts/Search System Is Partially Available	This messages notifies subscribers that not all fraud databases where available/checked for this transaction.	• One or more fraud databases were unavailable during the transaction.	• Rerun transaction at a later time. If problem persists, please notify TransUnion.	Medium/ High
9997	Clear/Clear For All Searches Performed	No high risk situations where detected by the service.	• No suspicious, high risk or known fraudulent SSNs, addresses nor phone numbers were detected based on the input or file identity data.	• Continue to the next step in your process.	Low
9998	IDVision Alerts/Search System Is Temporarily Unavailable	The service is not available at this time.	• The system is temporarily out of service.	• Rerun transaction at a later time. If problem persists, please notify TransUnion.	Medium/ High
9999	IDVision Alerts/Search System Access Not Authorized	The subscriber information used in the transaction is not authorized for this service.	• The subscriber code and/or password used in the transaction is not authorized to access the IDVision Alerts/Search solutions.	• Verify subscriber code and password, then rerun transaction at a later time. If problem persists, please notify TransUnion account manager.	N/A

