Technically Creative

Master Policy Catalog

3212 US Route 9W
New Windsor, NY 12553

GetInfo@TechnicallyCreative.com
www.technicallycreative.com

Table of Contents

Policy Overview

The Financial Industry Regulatory Authority (FINRA) rule 3010(a) states “Each member shall establish and maintain a system to supervise the activities of each registered representative, registered principal, and other associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable NASD Rules. Final responsibility for proper supervision shall rest with the member”. FINRA Rule 3010 essentially requires firms to maintain a system to supervise transactions and correspondence with their users. Companies should establish and maintain a supervisory system with written procedures, reviewing incoming and outgoing electronic communications on a regular basis.

The International Traffic in Arms Regulations (ITAR) outlines in § 120.27 (8) U.S. criminal statutes, Part 126 General Policies and Provisions, and Part 127 Violation and Penalties, the actions to be taken should such sensitive information be sent to unauthorized individuals or entities. This can include other non-registered firms, non-associated individuals, or individuals with potential ties with terrorist organizations. Communication surveillance is an integral tool that provides a secure defense to ensure minimal risk in terms of data loss prevention.

Policy is a fully customizable feature that defines the parameters, based on language content, by which an electronic communication is captured. Policies, using the concept of context in language, can control email, file, and Web activities in a client environment. By editing the parameters of a policy, clients have total flexibility to control and capture user behavior whether the purpose if for regulatory supervision or data loss prevention. Many communication surveillance applications focus on capturing keywords, however this method has the potential to yield an unmanageable quantity of results, which can make finding potential violations a “needle in a haystack” situation. Policy utilized the lingual concept of context to determine the meaning or value of a keyword. For example, the term “swap” in the financial vernacular is an agreement between two parties to exchange sequences of cash flows for a set period of time and is therefore a noun. In the Basic English vernacular a swap is a physical exchange and is most commonly used as a verb. Using policy’s capabilities of word proximity we can capture language around derivative swaps using the words around it that indicate it’s being used as a financial noun (e.g. his, her, that, LIBOR rate, EURIBOR rate, Plain Vanilla, Currency etc.) versus language that indicates it’s a plain English verb (i.e. swapping, make a swap, swap numbers, swap cards, he swapped). Using this principal, policy can also be used to recognize patterns such as a formatted phone number, credit card number, source code, Social Security numbers, etc.

Policy analyzes a document and based on the content scores a document according to a preselected and customizable score. There are 8 fully customizable parameters in policy that effect the scoring and how the policy scans the communication. Parameter 1 contains a set of prerequisites that are all required to be present in a communication before continuing to scan the communication. If one of these if found the score of the document is raised by one.

Parameter 2 contains a slight more specific set of prerequisites and policy where at least one must be present. If one is detected in parameter 2 the score of the document is raised by one. Parameter 3 contains the most specific language and anything present in this parameter will raise the score in accordance with how many matches are present in the communication. Parameter 4 contains negative indicators and if a match is found, policy will reduce the score by one for each instance. Parameter 5 contains a list of definite non-matches which, if any are matched, policy will abort the search and the event will not trigger. Parameter 6 contains the minimum score that will cause the policy to capture the event. Parameter 7 contains a list of keywords or phrases that can be used to generate a report based on the captured content. Parameter 8 is a list of definite matches that, if found, increases the score by 100.

Once the conditions of the policy have been met, and an event is captured, it is reviewed by a person who will determine if a violation has been occurred. If the conditions of the policy were met but the event contains language that is not pertinent to the intent of the policy, the event is placed in a queue to be looked by a policy refinement technician. This technician analyzes the event and refines the policy in order to prevent the event, or any similar event, from being captured. Policy refinement is a necessary and ongoing process as the criteria for what is and isn't a violation are constantly evolving.

General New Policy Release Process

Requirements Gathering

a. When a client determines that there is an assessed risk that can be mitigated by the creation of a policy, we work with the client to determine the focus of the policy.
    i. Who, what, where, when.
        1. Who is the policy being applied to (Globally, only to certain groups)? Who is being excluded from the policy (if anyone)?
        2. What content are we looking to capture? What is the overall objective of this policy?
        3. Where are we looking for this content? (Email subject, body, or attachment, in web activity, in a file on a share, sent to a printer?)
        4. When do we want this policy to apply? (When sent externally, one individual sends to another individual in a different department, when at least 1 external recipient is on the communication and an attachment is present?)
    ii. These requirements are gathered from the client at which point a policy architect will determine the final piece, how.

Development

b. Planning
    i. Once the client has conveyed what they'd like in a policy, the policy architect will determine the best course of action, in terms of what is the best way to build the policy, in order to achieve the requirements.
    ii. This plan is reviewed with the client to ensure that they agree with the approach.
c. Policy Development
    i. Once the client approves of the plan that has been laid out, the policy architect begins to build the policy in an in-house development environment.
    ii. Once this has been completed, we perform in-house testing in an environment that has been created to replicate that of the clients.
d. Client release documentation
    i. Once in house testing has been completed, the policy parameters are documented and distributed to the client for release into their environment.

UAT/Client Testing

e. From the in house Development Environment, the changes are then moved into the client's test environment. This is done by copying and pasting the changes from the documentation provided by the policy architect.
f. Specific processes relating to UAT testing are unique to the client.
g. Once client testing is completed, the final version of the policy is documented by the policy architect, and distributed to the client. Specific client documentation is also created at this time.

New Policy Release Document

h. Once the client has signed off on the functionality of the policy, the parameters of the policy are provided in the New Policy Release document:

New Policy Release Document

All aspects of the policy have been tested in a development environment. This document adheres to the template as outlined below.

Policy Name:	[Insert Policy Name Here]
Release Location:	[Geographic Location of CMS]
CMS Name:	[Name of CMS Release is occurring]
Apply to User Level:	[Navigation to Hierarchy user level. Change level noted in ""]
Policy Type:	[Doc Class, DIM, DAR, Capture, Web, Recipient etc]
[Class\File] Number:	[After Policy type is indicated, File/classification number]
Classification Number:	[Classifier number used if policy uses it] (Classification Name)
Navigation to the Policy:	[Location of policy in Policy Editor]
Requesting Entity:	[Group or Individual requesting the policy]

Policy Description: [Detailed policy description]

Policy Parameters:

- Trigger Name
- Policy Class
- Severity
- Smart Tags
- Which Address List?
- Included Addresses
- Excluded Addresses
- Ignored Addresses
- Encryption Filter
- Digital Signature Filter
- Which E-mail Sources?
- Data Lookup Command
- Data Lookup Failure Mode
- Sampling Rate
- Minimum Retention (Days) - Authorized Activity
- Minimum Retention (Days) - Prohibited Activity
- Control Action
- Message To Users
- Additional Trigger Configuration

Classification Parameters: [Optional]

i. This document outlines the granular details in an easy to read format for reference, release, and compliance purposes.
j. Since this is a technical document, a "plain English" catalog version is also written an distributed which outlines the purpose of the policy, how the policy achieves this purpose, and a simple explanation of the technical way the policy works, in order to achieve its purpose.
k. Once the client's review of the documentation is complete, the documents are then sent to the requesting bodies, at the client, for approval to release to production.

Production Release Process

l. Change Request
    i. Each Client varies, however we work with the client through the approvals that need to be attained before a release to production.
m. Release
    i. The changes are released to production by a designated individual.
    ii. After all of the changes are released, they verify that there are no errors reported in the activity log.

Post Release

n. The refinement document is delivered to the client for archiving purposes.
o. An XML export is taken to reference for rollback purposes for the next release.
p. A copy of the refinement document archived to a Technically Creative directory.

General Policy Refinement Process

Refinement Queue

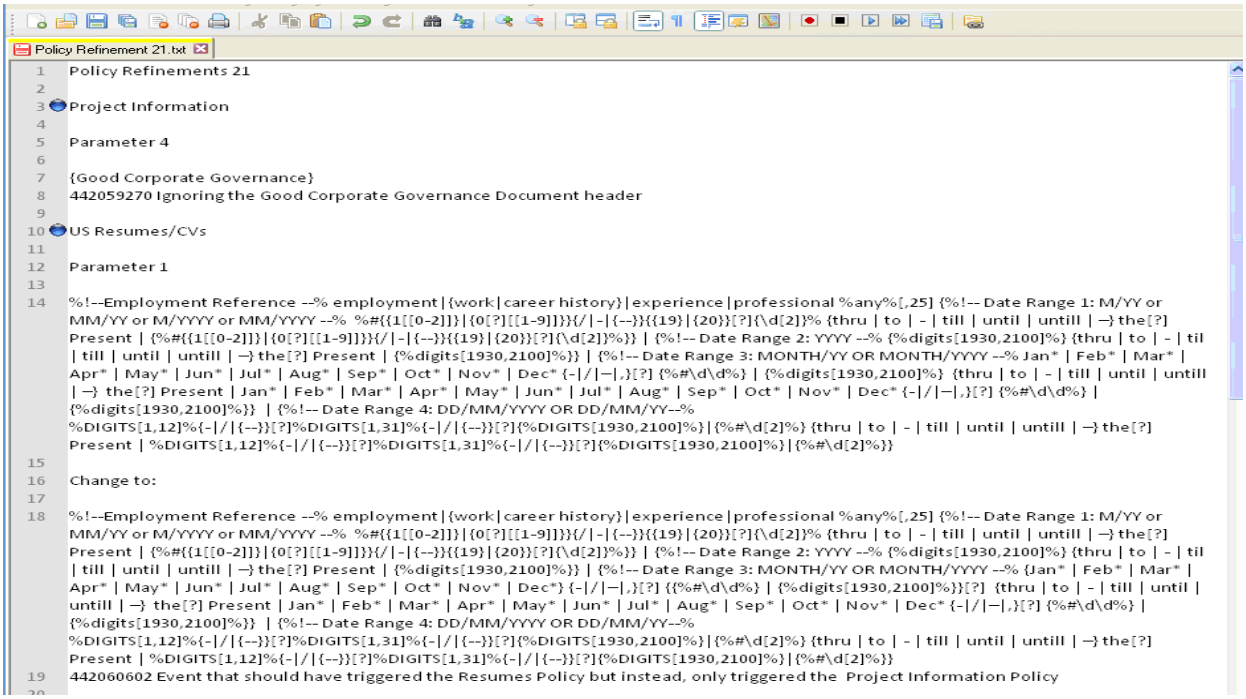
a. A policy technician goes through the refinement queue with a preferable date range set to only show the past 2 weeks' worth of events. This ensures that the events displayed are events that were still captured after the latest round of refinements because events older than a week might have already been refined out.

b. Alternatively, the events that require refinement are compiled by the client and sent to Technically Creative for the purpose of review and context.

c. Refinement notes are recorded in a Notepad++ document, based on the events viewed

   i. The format for the document is as follows. Note: There is no particular order regarding which Policies are refined.

      1. Policy name
      2. Line to be added, deleted, or changed
      3. Production EventID that references the event that the refinement applies to and the one it is tested against followed by a brief explanation of the intent of the line. Example:



   d. After the EventID has been recorded, the event is downloaded as an outlook file and placed on a separate drive, that's connected to a CMS, for testing.

Development Testing

e. Once the queue has been cleared and the events have been marked with an audit status to reflect that, I apply the refinement changes noted in the notepad document to the policies in a development environment.

f. Development Imports

   i. The first import that is done is against production data. This is done to ensure that there are no syntax errors present in the new round of refinements.

      1. If a syntax error is present, this is corrected in the notepad++ document and in development.

   ii. Once it is confirmed that there are no syntax errors, I run an import of the events that were downloaded into the separate drive, that's connected to a CMS, to ensure that none are captured

      1. If events are captured, further refinements are made and added to the Notepad document

   iii. When it's confirmed that there are no syntax errors and there are no events that are captured the changes are moved to UAT.

UAT Testing

g. The UAT Environment is constantly updated to mirror production. This includes policies, hierarchy, User Attributes, settings, policy roles, Policy classes, security models, user roles, and patches that have been applied to production.

h. From The Development Environment, the changes are then moved into UAT. This is done by copying and pasting the changes from the Notepad ++ document.

i. The configuration file is updated to reflect the date range that was covered by the refinement queue.

j. UAT Imports

   i. To ensure the most accurate test of the changes, all of the policies that are enabled in production are enabled in UAT. This is to see how the policies behave together.

   ii. The changes are run against production data that is imported via SQL import from.

      1. The activity log, performance monitor (items processed per second), hit ratio (Captured:Processed), event import log, and windows logs are all checked to verify that there are no errors or erroneous results.

         a. If there are errors these corrections are made to the Notepad ++ document to modify the strings.

iii. Once it's been confirmed that there are no errors present. The captured events are reviewed to determine the quality of what the policies have captured.
    1. Any additional, last minute refinements are made and added to the Notepad ++ document.
        a. These are typically minor changes (enhancements to current changes) that are tested right in UAT rather than development.
        b. Any major changes (syntax changes, added lines, changes to current strings) are tested in development and follow the same testing guidelines as previously outlined.

Policy Refinement Document

k. Once it is confirmed that there are no errors, the lines added successfully refined out the events, and there was no significant impact to the integrity of the policies the changes are then documented a Policy Refinement Document as outlined:

Policy Refinement Document

All refinement changes have been tested in a development environment. This document adheres to the template as outlined below.

Policy Name:	[Insert Policy Name Here]
Apply to User Level:	Navigation to Hierarchy user level. Change level noted in ""
Policy Type:	Doc Class, DIM, DAR, Capture, Web, Recipient etc
[Class\File] Number:	After Policy type is indicated, File/classification number
Classification Number:	[Classifier number used if policy uses it] (Classification Name)
Navigation to the Policy:	Location of policy in Policy Editor
Areas Being Changed:	[Areas being changed]
Summary of Changes by Area:	[Summary of changed/reason for changes]

Changes:

Area:	[Area being changed (e.g. Parameter 4, data lookup, Control Action)]
[Added/Deleted/Changed] Line:	**Specify actual added changed or deleted line**
Reason for Change:	*[If production event Include Event UID and description of line function]*

l. This document outlines the granular details in an easy to read format for reference, release, and compliance purposes.
m. The refinement document is then sent to the individual designated to do the release to double check and confirm that the changes in the document match what's in UAT.
n. Once their review is complete the document is then sent to the requesting bodies for approval.

Production Release Process

o. Change Request
    i. Each Client varies, however we work with the client through the approvals that need to be attained before a release to production.
p. Release
    i. The changes are released to production by a designated individual.
    ii. After all of the changes are released, they verify that there are no errors reported in the activity log.

Post Release

q. The refinement document is delivered to the client for archiving purposes.
r. An XML export is taken to reference for rollback purposes for the next release.
s. A copy of the refinement document is archived to a Technically Creative directory.

Recipient Policies

Communication with the Press/News Organizations

Companies often hire people specifically for public relations. These individuals have been trained to interact with news organizations in an effective and efficient manner and understand how to best portray the image that the company desires. Most importantly, these individuals understand what information should and should not be released to the public. It is therefore in a company's best interest to prevent unauthorized individuals from communicating with news organizations.

The Communication with the Press/News Organizations policy is intended, as the name implies, to monitor and capture unauthorized users from sending electronic communications to members of the press or individuals employed in a news organization. The policy works by analyzing a communication after it is sent to determine if any of the recipients are external addresses. Once the presence of an external address is identified, the policy then refers to a list of common news organization addresses to determine if any of the recipients are affiliated with the press. If a match is found, the event is captured and flagged for review by an individual who will determine the severity of the violation.

Communication with Regulatory, Legal, and Governmental Authorities

In a financial company there are individuals whose sole purpose is to communicate with and to maintain a positive working relationship with the regulators. Any information that is sent to them is reviewed extensively to ensure accuracy, relevance, and to promote a positive relationship between a firm and the authorities. This policy does not monitor for whistle blowing, but strictly ensures that only authorized individuals communicate with any regulator or government authority. The Communication with Regulatory, Legal, and Governmental Authorities policy is intended to monitor and capture surveilled user's attempts to contact or otherwise communicate with government entities.

The Communication with Regulatory, Legal, and Governmental Authorities works by analyzing a communication as it is sent to determine if any of the recipients are external. If an external address is detected, the policy will then compare the address to a list of possible government or regulatory addresses. Once an address is matched to one on the list, the policy captures the event and flags it for review by an individual who will determine the severity of the infraction.

Sending to Personal Addresses

The Sending to Personal Addresses policy is a DLP (data loss prevention) policy. As opposed to the out of the box E-mail to Personal Addresses policy that uses a black list establishing a list of addresses that cannot be recipients, this policy uses a white list to determine a set of email addresses that are not considered violations. This is due to the fact that a personal email address is not limited to simply hotmail, yahoo, gmail etc. This method ensures that any message sent to an address that is not on this list is captured.

The policy works by analyzing an email to determine whether it is internal or external. Once the policy confirms that it is outbound, it will then confirm that the message contains at least one attachment. If an attachment is found, the policy then confirms that the total message size is greater than 15kb (this is to prevent signature logos from being captured). When it confirms the message size, it then analyzes the list of recipients to ensure that the addresses are on the white list. If an address is not on the white list, policy will verify if any other recipient is on the list. If another recipient is on the list, then the event will not capture. So, to summarize, the conditions in which an email is captured are as follows:

- The message is sent externally
- The message contains at least one attachment
- The total size of the message is greater than 15kb
- None of the recipient addresses are on the white list (The message will not capture if a white listed address is present)

Once all of these conditions are met, the policy captures the event and flags it for review by an individual who will determine the level of severity.

Document Classification Policies

Account Number

As outlined in the Gramm-Leach-Bliley Act, companies defined under the law as "financial institutions" are required to ensure the security and confidentiality of customer information such as Social Security numbers, credit histories, addresses, phone numbers, bank and credit card account numbers. Individual states such as Massachusetts have also passed laws such as The Standards for the Protection of Personal Information of Residents of the Commonwealth that establish standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objective of these laws is to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards, to protect against anticipated threats of hazards, and to protect against unauthorized access to or the use of such information that may result in substantial harm or inconvenience to any consumer.

The Account Number policy analyzes communications for number strings that resemble bank issued account numbers. Unfortunately, account numbers vary in length and general format, and there is no definite standard by which to establish that a given number is, in fact, an account number. However, the policy compensates for this obstacle by searching communications for language that would indicate that an account number is present. Such indications include words and expressions like "A/N", "Account #", or "Acct num" etc.

The Account Number trigger first searches for prerequisite qualifiers such as the literal mentioning of "telephone number", "fax number", "tracking", or the mention of an account number, all in combination with any sequence of 4 to 12 digits optionally preceded by 3 to 4 letters. Once these general and non-specific conditions are met, the trigger then focuses on specifically targeting the most common way in which account numbers can be structured. If the policy finds a match then the trigger fires and the event is flagged for review to determine if there is a violation.

Account Number – Threshold

As outlined in the Gramm-Leach-Bliley Act, companies defined under the law as "financial institutions" are required to ensure the security and confidentiality of customer information such as Social Security numbers, credit histories, addresses, phone numbers, bank and credit card account numbers. Individual states such as Massachusetts have also passed laws such as The Standards for the Protection of Personal Information of Residents of the Commonwealth that establish standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objective of these laws is to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards, to protect against anticipated threats of hazards, and to protect against unauthorized access to or the use of such information that may result in substantial harm or inconvenience to any consumer.

The Account Number - Threshold policy analyzes communications for a specified number, or threshold, of common bank issued account numbers. Account numbers vary in length and general format and there is no definite standard by which to establish that a given number is, in fact, an account number. This policy, however, compensates for this obstacle by searching communications for language that would indicate that an account number is present. Such indications include words and expressions like "A/N", "Account #", or "Acct num" etc. The Account Number - Threshold policy is specifically tailored to capturing events containing multiple account numbers as this can be indicative of an individual attempting to distribute a client list populated with confidential customer data.

The trigger first searches for prerequisite qualifiers such as the literal mentioning of "telephone number", "fax number", "tracking", or the mention of an account number, in combination with any sequence of 4 to 12 digits optionally preceded by 3 to 4 letters. Once these general and non-specific conditions are met, the policy continues to search for more specific and commonly used structures for an account number. The Account Number - Threshold policy requires a customer defined minimum, or threshold amount, of account number matches before the trigger fires. Once an event is captured it is flagged for review by a designated person who determines if the hit is an actual violation.

Account Number and Routing Information

As outlined in the Gramm-Leach-Bliley Act, companies defined under the law as "financial institutions" are required to ensure the security and confidentiality of customer information such as Social Security numbers, credit histories, addresses, phone numbers, bank and credit card account numbers. Individual states such as Massachusetts have also passed laws such as The Standards for the Protection of Personal Information of Residents of the Commonwealth that establish standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objective of these laws is to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards, to protect against anticipated threats of hazards, and to protect against unauthorized access to or the use of such information that may result in substantial harm or inconvenience to any consumer. Additionally, Federal Regulation J, Article 4A of the Uniform Commercial Code (UCC), The Payment Card Industry Security Standards Council Regulations (PCI) and FDIC Regulation 6500 Title IX (Electronic Fund Transfer Act) outline the various requirements regarding the procedures involved in wire transfers. Federal Regulation J and the Electronic Fund outline the procedures by which transfers need to occur to ensure the security of the customer's information. The PCI standard states the requirement for encryption of any electronically transmitted payment card information whether at a terminal such as an ATM, or sending the physical information through electronic communication. Article 4A of the UCC defines "security procedure" as "a procedure established by agreement of a customer and a receiving bank for the purpose of verifying that a payment order or communication amending or cancelling a payment order is that of the customer" and "may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices."

While the Unencrypted Wire Transfer Information policy focuses specifically on the mention of a formal bank wire transfer (i.e. sending legitimate information but perhaps forgetting to encrypt it), the Account Number and Routing Information policies searches for many of the same alpha-numeric string features as noted in Unencrypted Wire Transfer, but concentrates on bank routing/ABA/ACH numbers. This provides a more general yet comprehensive policy that is complementary to Unencrypted Wire Transfer Information.

The Account Number and Routing Information trigger scans a communication for the mention of either the term “routing number” within 50 words of a possible number combination indicative of an ABA routing number, or the mention of an ABA or ACH routing number in the vicinity of possible number combinations that would match an ABA routing number. Once either of these matches is found, the trigger continues to scan for various number combinations that could be an account number such as 2 digits dash 16 digits, or mention of “account number” near a 6 to 18 digit number (but will ignore a 7 or a 10 digit number that follows a telephone number pattern). Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Account Number with Additional PII (Personally Identifiable Information)

As outlined in the Gramm-Leach-Bliley Act, companies defined under the law as "financial institutions" are required to ensure the security and confidentiality of customer information such as Social Security numbers, credit histories, addresses, phone numbers, bank and credit card account numbers. Individual states such as Massachusetts have also passed laws such as The Standards for the Protection of Personal Information of Residents of the Commonwealth that establish standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objective of these laws if to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards, to protect against anticipated threats of hazards, and to protect against unauthorized access to or the use of such information that may result in substantial harm or inconvenience to any consumer.

The Account Number with Additional PII policy analyzes communications for common bank issued account numbers. Account numbers vary in length and general format and there is no definite standard by which to establish that a given number is, in fact, an account number. This policy, however, compensates for this obstacle by searching communications for language that would indicate that an account number is present. Such indications include words and expressions like "A/N", "Account #", or "Acct num" etc. The specific purpose of the Account Number with Additional PII policy is to capture attempts to divulge account details along with information that can identify, and cause substantial harm, to an individual.

The Account Number with Additional PII trigger first searches for prerequisite qualifiers such as the literal mentioning of "telephone number", "fax number", "tracking", or the mention of an account number, in combination with any sequence of 4 to 12 digits optionally preceded by 3 to 4 letters. Once these general and non-specific conditions are met, the policy then searches the communication for information that can identify an individual such as an address, a phone number, a date of birth, or column headers that are typically found on a spreadsheet containing such information. The trigger then continues to scan the communication for more specific and commonly used structures for an account number. If an account number match is confirmed then the trigger fires and the event is flagged for review by a designated reviewer to determine if there is a violation.

Anti- Money Laundering – OFAC

"Money Laundering" is defined as the process whereby the proceeds of crime are transformed into ostensibly legitimate money or other assets, or the process by which the true origins of money is concealed in order to make it appear legitimate. FINRA, the SEC, the NYSE, the CFTC, as well as numerous acts such as the Bank Secrecy Act and the Patriot Act have all established regulations around the prevention of money laundering activities for various reasons. To enforce these regulations, FINRA Rule 3310 states that "Each member shall develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member compliance with the requirements of the Bank Secrecy Act (31 U.S.C. 5311 et seq.) and the implementing regulation promulgated thereunder by the Department of the Treasury." In addition, the Office of Foreign Asset Controls (OFAC) administers and enforces economic and trade sanctions against foreign entities based on US foreign policy. Currently, these sanctions, of varying degrees, have been imposed on Cuba, North Korea, Iraq, Iran, Burma, Sudan, The African Diamond Trade, The Balkans, Zimbabwe, Syria, Côte D'ivore, Belarus, The Democratic Republic of Congo, and Somalia.

Based upon requirements set forth by OFAC, the Anti-Money Laundering - OFAC policy is designed to identify electronic communications concerning the countries and cities enumerated on the OFAC Sanctions and Country list, in combination with language indicative of an illicit transfer.

The Anti-Money Laundering – OFAC trigger works by first identifying common methods of laundering money such as language around money, stock, bond, or fund transfers, third party transfers, travelers checks, or suspicious activity reports. Once the policy matches one of these pre-qualifiers, the trigger continues to scan the communication for things such as countries on the OFAC sanctions list, language around the concealing process such as "Transfer the money to the shell company", "Washing the assets", or deceptive language such as "Top secret", "We're going to have to do this under the radar", or "This shouldn't raise any red flags". When a customer-determined threshold of matches is reached, the trigger fires and flags the event for review to determine the level of severity.

Attorney Client Privilege

“The principle of confidentiality is set out in the legal ethics rules in each jurisdiction and in the ABA Model Rule 1.6. Model Rule 1.6 Comment [2] stated: 'A fundamental principal in the client –lawyer relationship is that in the absence of the client’s informed consent, the lawyer must not reveal information relating to the representation. … This contributes to the trust that is the hallmark of the client-lawyer relationship.' A violation of the ethics rule may lead to disciplinary sanctions.” This regulation is part of the American Bar Associations ethics law around attorney client privilege, essentially stating that a lawyer cannot divulge client information relating to legal cases without the explicit permission granted by the client to do so. This also protects the attorney, as he/she are not held under any legal obligation to divulge information that is covered under this law. Violation of this rule can result in not only disbarment of the individual that provided such information, but also reputational damage to the firm and legal action being taken by the client.

The Attorney Client Privilege policy captures communications that may contain sensitive information that could violate attorney client privilege. This privilege extends to any correspondence, but once that information is transmitted out of your company the privilege is waived. Consequently protecting this privilege and preventing the transmission of this information is a necessity.

The Attorney Client Privilege trigger scans for specific phrases that could indicate the violation of the American Bar Associates ethics law. Such phrases include “Memorandum of Counsel”, “The opinion of counsel is…”, or “Communication of counsel”. Once a customer defined threshold of matches is reached the trigger fires and flags the event for review to determine the severity of the offense.

Australian Medicare Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Australian Medicare Card Number policy captures the unauthorized distribution and dissemination of Australia's version of the Social Security number in the United States. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Australian Medicare Card Number policy works by first identifying the mention, or otherwise labeling, of the information in a given communication ("Medicare card", "medicareaustralia"). Once a match is identified, the policy continues its search for a Medicare card number, which is done by using a pattern matching definition tailored to identify the basic format of an Australian MCN. Once the policy identifies both of these pieces in a communication, the policy flags the event for review by an individual to determine the severity of the offense.

Australian State Driver's License

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

Similar to the UK Driver's License and the US Driver's license policies, the Australian State Driver's License policy is designed to look for individuals unlawfully distributing sensitive client information, which is typically contained in a driver's license.

The Australian State Driver's License policy works by first scanning a communication either for the mention of a driver's license ("License Number", "DL State", "Driver's License"), or a type of license, such as a CDL. Once this condition is met, the policy uses a pattern matching definition to identify Australian driver's license numbers in various formats. When these conditions are met, the policy triggers the event and flags it for review by an individual.

Australian Tax File Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Australian Tax File Number policy captures the unauthorized distribution and dissemination of Australia's version of the United Kingdom's Tax Identification Number. This is designed to ensure the safety of the information that is entrusted to a company.

The Australian Tax File Number policy works by first identifying the mention, or otherwise labeling, of the information in a given communication ("TFN","Tax file number/no/#"). Once a match is identified, the policy then continues its search for a Tax File Number, which is done by using a pattern matching definition tailored to identify the standard format of an Australian TFN. Once the policy identifies both of these in a communication, the policy flags the event for reviewed by an individual to determine the severity of the offense.

Background Checks

Multiple regulations exist to establish a level of protection for an individual's personally identifiable information. These include, but are not limited to, HIPAA, FCRA, and the Privacy Act of 1974 in the United States, PIPEDA in Canada, or the Directive on the Protection of Personal Data in the European Union. Each of these regulations define what is considered personal information, and broadly state that the information collected by an individual cannot be disclosed to other organizations or individuals unless authorized by law or by consent of the individual.

The Background Checks policy attempts to prevent the unlawful distribution of sensitive data, specifically background check information as specified as part of the United States Equal Employment Opportunity Commission's set of regulations.

The Background Checks policy first searches for a date of birth, as this is a required part of any background check. Once the a date of birth is identified, the policy continues searching for specific phraseology to indicate an "application", "Investigate Background Inquires", "Personal History", and other contextual phrases that are typically found on a background check application. If the message fulfills these two requirements, the policy then searches for specific information that would be considered a violation, including Driver's License numbers, Social Security Information, "Credit history/checks", or the mention of misdemeanors and other types of legal offenses. Once these conditions are met, the policy triggers and flags the event for review by a designated person to determine if the event is a violation.

Benchmark Interest Rates

In light of the relatively recent events regarding the London Interbank Offering Rate (LIBOR) manipulation and in response to the new LIBOR regulations established by the UK Financial Services Authority, and the general supervision of benchmarks, the Benchmark Interest Rate policy was created. The BIR policy covers not only LIBOR rates, but other rates that have been, or could potentially be, subject to manipulation. This policy monitors individuals in the firm who are not designated rate setters discussing big rigging, LIBOR manipulation, the manipulation of other interbank offering rates (i.e. TIBOR, EURIBOR, JIBOR), or general discussions of the manipulation of any of these various rates.

The Benchmark Interest Rate policy analyzes a communication for a variety of terms relating to interbank offering rates, such as the mention of "LIBOR", "ERUIBOR", "Ruonia", "EOD GILT", "Japan Securities Clearing Corporation", or a general mention of fixing a rate. In addition to this set of terms, the policy also searches for terms relating to FX trading such as "USD USD", "closing bell", "prior to the bell", or "Fixing the 6mth". Once either of these two categories of pre-qualifiers are met, the policy then continues to search the communication for more specific terms or phrases such as "can u drop the 6 month EOD GILT", "Let's move it down 3 (or any number) bps", "u need lowest fix today?", or "Don't make this obvious". The policy is also designed to specifically target language around the manipulation of foreign exchange (FX). FX language examples include mentioning "Pre hedging", "LHS" or "RHS", "Fix Window", "Move (or mv) the Market (or mkt}", "Squeezing the client", and other contextual phrases such as the word "bang" within proximity of "CLS", the word "Stop" or "Stops" in proximity of "Taken out", "lower", "higher", or "Entry to buy/sell". Included in the FX monitoring portion of the policy are various commonly traded currencies and their abbreviations such as "USD" "US Dollar", "AUD" "Australian Dollar", "GBP" "British Pound", "TRY" "Turkish Lira", or "EUR" "Euro". When a predetermined threshold of matches is reached, the trigger fires and flags the event for review by an individual to determine the level of offense.

Benefits Enrollment Information

As outlined in §164.306 of the Health Insurance Portability and Accountability Act (HIPPA), covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce.

Since the advent of HIPAA, the disclosure of medical information is tightly controlled. To address this concern the Benefits Enrollment Information trigger scans for context and specific key words that indicates the user is sending confidential health information. Since this can present multiple legal issues for any business, it's critical that this trigger is robust yet flexible. The trigger can discern between solicitations and requests for information, and actual benefits enrollment information in both the message body and any attachments

The Benefits Enrollment Information trigger first identifies any literal mention of benefits enrollment, change in insurance plan, enrollment forms or applications, or health illustrations (such as x-rays, etc.). Once the policy confirms the presence of any of those prerequisites, the trigger continues to search the document for language pertaining to a detailed change to a plan, such as “I want to add my family to my plan”, “The mid-year enrollment is coming up”, or “I need to claim my reimbursement”. The trigger also looks for common field names and options found on a standard enrollment form such as add or drop a dependent, coverage level option, or effective date. If the policy finds a match it fires and flags the document for review by a designated person to determine if the event is a true violation.

Bid Rigging Detection: Insurance

Big Rigging is a form of fraud in which a contract is promised to one party even though, for the sake of appearance, several other parties also present a bid. This form of anti-competitive collusion is illegal in most countries as demonstrated under Section 1 of the Sherman Anti-Trust Act in the United States, Section 47 of the Canadian Competition Act, The Enterprise Act in the United Kingdom, and the Japanese Anti-Monopoly Law.

There are many different methods, terms, and situations in which bid rigging can occur. The Bid Rigging Detection: Insurance policy captures communications where individuals are attempting to rig a bid associated with the insurance industry, or insurance-associated instruments or contracts.

The Bid Rigging Detection: Insurance policy works in three steps. The policy first searches for a broad mention of terms such as a contract, Insurance, or Insurance Issuer. Once a match is found, the policy continues to the second level, where it searches for actions and items, which are associated with auctioning or bidding, including “Bids”, “Contracts”, and “GIC/Guaranteed Investment Certificate”. With a match here, the policy moves to the last stage where it searches for language associated with the action of rigging a bid such as “Beating to get to the contracts”, “Anti-Competitive”, “awarding you the contract”, and “In your favor”. Once these conditions are met, the trigger fires and flags the event for review to determine the severity of the violation.

Bid Rigging Detection: Municipal Bond Issuance

Big Rigging is a form of fraud in which a contract is promised to one party even though, for the sake of appearance, several other parties also present a bid. This form of anti-competitive collusion is illegal in most countries as demonstrated under Section 1 of the Sherman Anti-Trust Act in the United States, Section 47 of the Canadian Competition Act, The Enterprise Act in the United Kingdom, and the Japanese Anti-Monopoly Law.

There are many different methods, terms, and situations in which bid rigging can occur. The Bid Rigging Detection: Municipal Bond Issuance captures communications where individuals are attempting to rig a bid associated with a debt security issued by a municipality.

The Bid Rigging Detection: Municipal Bond Issuance policy works in three steps. The policy first searches for a broad mention of Municipal, Bond, or Underwriting. Once a match is found, the policy continues to the second level, where it searches for actions and items, which are associated with auctioning or bidding, including “Bids”, “Contracts”, and “GIC/Guaranteed Investment Certificate”. With a match here, the policy moves to the last stage where it searches for language associated with the action of rigging a bid such as “Beating to get to the contracts”, “Above the market”, and “In your favor”. Once these conditions are met, the trigger fires and flags the event for review to determine the severity of the violation.

Board Minutes and Discussions

At board meetings members often discuss sensitive topics with the expectation of confidentiality even though the meeting minutes are recorded. Further, these minutes can contain information relating to the status of the business, new ideas, and discussions relating to the plan or direction of a company. Ensuring the security of this information is a priority as it can cause potentially devastating repercussions. Using email surveillance, a company can monitor correspondence sent by users and prevent employees from distributing such information to unauthorized individuals.

The Board Minutes and Discussions trigger protects the confidential correspondence among board members, including minutes from official meetings and discussions, by scanning for words and phrases that identify meeting minutes, votes, polls, executive agenda, etc.

The Board Minutes and Discussions trigger first analyzes an email for certain prequalifying traits such as the mention of “The minutes of the meeting”, “Board of Directors”, or “Meeting agenda”. Once these are found, the policy continues looking for language that would be found in meeting minutes such as “The motion was seconded and passed”, “Meeting summary”, or “The meeting was adjourned”. Upon meeting a customer defined threshold of matches, the trigger captures the event and flags it for review by a person who will determine if the event is egregious.

Bribes/Kickbacks/Quid Pro Quo/Blackmail

The US Bank Bribery law 18 U.S.C. 215 states that “Whoever (1) corruptly, gives, offers, or promises anything of value to any person, with intent to influence or reward an officer, director, employee, agent, or attorney of a financial institution in connection with any business or transaction of such institution; or (2) as an officer, director, employee, agent, or attorney of a financial institution, corruptly solicits or demands for the benefit of any person, or corruptly accepts or agrees to accept, anything of value from any person, intending to be influenced or rewarded in connection with any business or transaction of such institution; shall be fined under this title or three times the value of the thing given, offered, promised, solicited, demanded, accepted, or agreed to be accepted, whichever is greater, or imprisoned not more than 30 years”. “Blackmail” is defined as the crime of threatening to reveal embarrassing, disgraceful or damaging information about a person to the public, family, spouse or associates unless money is paid to purchase silence. The UK Theft Act of 1968 section 21 states “(1) A person is guilty of blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces; and for this purpose a demand with menaces is unwarranted unless the person making it does so in the belief—
(a) That he has reasonable grounds for making the demand; and (b) that the use of the menaces is a proper means of reinforcing the demand. (2) The nature of the act or omission demanded is immaterial, and it is also immaterial whether the menaces relate to action to be taken by the person making the demand. (3)A person guilty of blackmail shall on conviction on indictment be liable to imprisonment for a term not exceeding fourteen years.”

This policy scans the communications of surveilled users for language that may indicate unsavory or under the table behavior with the intent being to prevent surveilled users from committing a criminal act before it occurs. This policy covers a broad range of language making it ideal to monitor, not just for acts of bribery and blackmail, but of deceptive language in general.

The Bribes/Kickbacks/Quid pro Quo/Blackmail trigger works by analyzing a communication for language that implies a “this for that” intent. Samples of quid pro quo (Latin for “something for something”) include phrases such as “You scratch my back I’ll scratch yours”, “One hand washes the other”, “Hush money”, or “This information is valuable”. The trigger also searches for sword-of-Damocles language such as “Pay me to keep me quiet”, “Do we understand one another”, or “You leave me with no other choice”. Once a customer-determined threshold of matches is found, the trigger flags the email further review.

Broker Error

FINRA Rule 4530 outlines the reporting requirements for Broker Dealers and states that each member shall promptly report to FINRA within 30 days if the member knows or should have known of the existence of a security violation, is named as the defendant in a regulatory case, is denied registration or expelled from becoming associated with any regulatory or self-regulatory body, or is subject to a statutory disqualification. That is to say, if an error is discovered which can lead to regulatory repercussions, it is required under this rule to be reported.

The Broker Error policy captures activity relating to such errors, to ensure the matter is brought to the attention of compliance, or other relevant parties, and that it is handled in the proper manner.

The Broker Error policy works by first identifying language associated with financial transactions such as “Stocks”, “Bonds”, “Mutual Funds”, or financial actions such as “withdraw”, “deposit”, or “call/put”. Once the mention of a financial instrument or transaction is identified, the policy continues searching the communication for language that indicates a mistake was made, or a transaction was done in error. Phrases such as “Reverse the transaction”, “Not done properly”, “issue on our part”, and “messed up the trade”, will breach the policy threshold and thus flag the event for review.

Canadian Social Insurance Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Canadian Social Insurance Number policy captures the unauthorized distribution of personally identifiable information, as it pertains to Canadian Social Insurance Numbers.

The Canadian Social Insurance Number policy works by first pattern matching a potential social insurance number, either formatted or unformatted. Once a match is identified, the policy then searches for an instance of formatted insurance numbers, or the identification of the number being a social insurance number, by looking for words such as "SIN", "Canadian Tax ID", or "numéro d'assurance sociale". When these conditions are met, the trigger fires, and flags the event for review by an individual to determine the severity of the violation.

Canadian Social Insurance Number - Threshold

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Canadian Social Insurance Number – Threshold policy captures the unauthorized distribution of personally identifiable information, as it pertains to Canadian Social Insurance Numbers. This threshold version is specifically used to capture multiple instances, as in the case of individuals disseminating client lists, database exports, or spreadsheets containing sensitive information.

The Canadian Social Insurance Number – Threshold policy works by first pattern matching a potential social insurance number, either formatted or unformatted. Once a match is identified, the policy searches for a specific threshold amount of formatted insurance numbers, or the identification of the number being a social insurance number by looking for words such as "SIN", "Canadian Tax ID", or "numéro d'assurance sociale". Once the predetermined threshold is met, the policy flags the event for review by an individual.

Canadian Social Insurance Number with Additional PII

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Canadian Social Insurance Number with Additional PII policy captures the unauthorized distribution of personally identifiable information, as it pertains to Canadian Social Insurance Numbers in conjunction with other personally identifiable information.

The Canadian Social Insurance Number with Additional PII works by verifying that a communication contains a match to the Canadian Social Insurance definition. Once a match is identified, the policy searches for the mention of information such as date of birth, generic column headers, postal codes, or other indications of a generic address. If these pre-qualifiers are met, the policy searches for a mention of "ID number", forms that would contain the aforementioned information, or other use cases for the information (i.e. tax returns). Once all three of these conditions are met, the policy triggers and flags the event for review by an individual to determine the severity of the violation.

Chinese Identity Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Chinese Identity Card Number policy captures the unauthorized distribution and dissemination of China's version of the United States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Chinese Identity Card Number policy works by utilizing policy's pattern matching capabilities to identify an Identity Card Number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Chinese Identity Card Number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of a Chinese ICN. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Client Technical Data

For companies dealing with confidential technical specifications, network designs, infrastructure configuration, and various other forms of sensitive technical information, their protection and security is of paramount importance. In order to avoid detrimental network security breaches, aggressive government regulatory repercussions, reputational damage, and loss of customers, for both your company and your clients', it's necessary to protect the information that your company has been trusted with.

The Client Technical Data policy is an enhanced version of both the Technical Specifications and Designs and Internal IT Support Documents policies. Its focus is to capture the discussion or distribution of any type of technical information, be it client or internal.

The Client Technical Data policy works by first identifying terms that are indicative of Network configurations ("IP Address", "Server name", or "TCP Port"), Technical Support ("Run install wizard"), or Network Security ("Packet sniffing", "Cracking"). Once a match is identified, the policy searches for more specific terms and patterns relating to the labeled information that was previously matched, such as IPv4 and IPv6 Addresses, MAC addresses, Router brands, or file paths. When a predetermined threshold is breached, the policy flags the event for review by an individual.

Coercive Behavior and Intimidations

Coercion and intimidation come in a variety of forms and as a result there are various regulations that ensure against the use of intimidation, aggressive force, or coercion. Such established laws include 24 C.F.R. 100.400 regarding housing and urban development, 25 C.F.R. 31.6 governing coercion with school district transfers, 39 C.F.R. 447.61 intimidation of postal service employees, 18 C.F.R. 706.210 regarding government employees using their position to coerce or intimidate, and 18 C.F.R. § 594 prohibiting voter intimidation. In the financial industry, FINRA Rule 5240 (a) states "No member or person associated with a [financial institution] shall: (3) engage, directly or indirectly, in any conduct that threatens, harasses, coerces, intimidates or otherwise attempts improperly to influence another [financial institution], a person associated with a [financial institution], or any other person. This includes, but is not limited to, any attempt to influence another member or person associated with a member to adjust or maintain a price or quotation, whether displayed on any facility operated by FINRA or otherwise, or refusals to trade or other conduct that retaliates against or discourages the competitive activities of another market maker or market participant."

Without considering the number of regulations on the topic, achieving goals and objectives through the use of coercion, aggressive threats, and intimidation, is generally a poor business practice. The Coercive Behavior and Intimidation policy is an all-encompassing, general blanket policy that monitors surveilled users' attempts to use non-specific threatening or aggressive language.

The Coercive Behavior and Intimidation trigger, as previously mentioned, looks for non-specific attempts to coerce and intimidate such as "You should be afraid of me", "Do not test me", "I will put your family in danger", or "Nothing will happen to you as long as you…". Once a customer-determined threshold of matches is reached, the trigger fires and flags the event for review to determine the severity of the infraction.

Confidential Trade Data

Private firms who are contracted to the U.S. government, regardless of services rendered, are subject to 18 U.S. Code § 1905, which states that "Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Federal Housing Finance Agency, or agent of the Department of Justice as defined in the Antitrust Civil Process Act, or being an employee of a private sector organization who is or was assigned to an agency under chapter 37 of title 5, publishes, divulges, discloses, or make known in any manner or to any extent not authorized be law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerned or related to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment." This regulation expresses a need for firms that do business with government agencies to monitor the communication of employees to ensure the security of such information. Likewise, any enterprise environment contains confidential information regarding trade secrets or just general data that is classified as company confidential. This creates a need for communication surveillance, not just for companies affiliated with the government, but for any company that wants to ensure the security of their data.

The Confidential Trade Data policy prevents the transmission of trade information, trade secrets and proprietary information for both companies that are affiliated with government agencies and firms that simply have a desire to implement a viable data loss prevention solution. This trigger scans for language indicative of trade details, as well as standard phraseology that would identify a confidential message.

The Confidential Trade Data trigger does not look for the data itself, as this is too varied, but for language that indicates the data is confidential. Typically, in a document of such importance and classification, there are disclosures that inform the user "The information contained herein, is confidential", "Not to be distributed except with the sole authorization of the author or owner", or "This information is not approved for distribution or circulation". The trigger targets these phrases, and such similar phrases, and when a customer defined threshold of matches is met, the policy flags the event for review to confirm the validity of the hit. This policy, as all of the others, can be adjusted, refined, or altered by a policy technician to capture specific information, or additional data at the request of the client.

Corporate Contracts

Corporate contracts are written agreements by which the legal parameters and conditions regarding employment, sales, tenancy, or other business arrangements between two or more parties are specifically outlined. Due to the nature of these contracts, the subjects that they contain are often sensitive in nature and therefore not considered part of the public knowledge domain. Ensuring the security of such documents becomes of paramount importance when such contracts contain information that could be used for illicit trade, investments, or other activities that could potentially violate the rules and regulations around inside information and its use thereof. Email Surveillance provides a comprehensive data loss prevention solution geared to minimize the risk associated with the unlawful distribution of such documents.

The Corporate Contracts policy is designed to capture the attempts of surveilled users to distribute corporate contracts which may contain sensitive non-public information. The policy is generally used to monitor who sends what and where it is being sent to, as often times the transmission of contracts is a necessary business function.

The Corporate Contracts trigger works by analyzing a communication for the presence of key words, phrases, and types of information typically found in such documents such as "witnesseth", "The counterparties agree to…", "Severability", or use of the terms "contract" or "entire agreement". Once a customer-determined threshold of matches is identified, the event is captured and flagged for review by someone to determine the severity of the violation.

Corporate Criticism

It can be argued that reputation is the greatest asset that a company has. When an employee speaks in a negative manner about the company, this can have a severely damaging impact on that company's reputation. In addition to being generally distasteful, speaking poorly of your employer, manager, or a company is unprofessional and can ruin an employee's reputation as a result. The Corporate Criticism policy captures communications that criticizes the company, its products, or members of management. By ensuring that these comments are captured, a company ensures that the reputation of the company and the employee are not damaged and it maintains a positive professional work environment.

The Corporate Criticism trigger works by analyzing a communication for the presence of criticizing language such as "The performance around here is awful", "The managers around here are crap", or "It makes this company look incompetent". The trigger also identifies language that indicates intent to resign such as "I can't take it at this job any more", "I really hate working here", or "I can't stand who I'm working for". Once a customer-determined amount of matches occurs the trigger fires and flags the event for review.

Credit Card Information

The Data Security Standard, a proprietary information security standard developed by the Payment Card Industry (PCI), outlines the requirements for handling credit card information. The twelve requirements, each specifically outlined to maintain PCI compliance, include the prerequisites to install and maintain a firewall configuration to protect cardholder data; to protect stored cardholder data; to encrypt transmission of cardholder data when sent across open, public networks; to develop and maintain secure systems; to restrict access to cardholder data based on business "need-to-know"; to track and monitor all access to network resources and cardholder data; and to maintain a policy that addresses information security.

The Credit Card Information policy attempts to protect sensitive client information and maintain PCI compliance standards by capturing emails and other forms of electronic communications that contain valid credit card numbers.

Credit card numbers are validated for authenticity using the Luhn (modulus 10) algorithm so that a random sixteen digit number will not trigger the policy, thus resulting in a reduction of false positives. Additionally this trigger specifically looks for standard credit card names such as American Express, Visa, MasterCard etc., as well as expirations dates, PIN Numbers, and CVV Security codes.

When the policy analyzes a communication it creates a score based on its content. A communication must contain a valid credit card number and another piece of information that is found on a card. For example: “0123 4567 8901 2345 CVV 123” will not capture because the card number is not valid according to the Luhn algorithm. However “The number is 4511 8701 2166 5236 exp. date 4/17” will get a score due to the presence of a valid credit card number and the presence of an expiration date. These two pieces of information raise the score of a given communication which fires the trigger and flags the event for review to determine if a violation actually occurred.

Credit Card Information – Threshold

The Payment Card Industry (PCI) Data Security Standard is a proprietary information security standard that outlines the handling requirements for credit card information. The twelve requirements, each specifically outlined to maintain PCI compliance, include the prerequisites to install and maintain a firewall configuration to protect cardholder data; to protect stored cardholder data; to encrypt transmission of cardholder data when sent across open, public networks; to develop and maintain secure systems; to restrict access to cardholder data based on business "need-to-know"; to track and monitor all access to network resources and cardholder data; and to maintain a policy that addresses information security.

The Credit Card Information - Threshold policy attempts to protect sensitive client information and maintain PCI compliance standards by capturing emails and other forms of electronic communications that contain valid credit card numbers.

Credit card numbers are validated for authenticity using the Luhn (Modulus 10) algorithm so that a random sequence of 16 digits will not cause the trigger to fire, thus resulting in a reduction of false positives. The Credit Card Information – Threshold policy analyzes an email based on the same standards as the Credit Card Information policy but allows the presence of a specified amount of credit card numbers (a threshold amount) before capturing a communication. The client defined threshold specifically targets attempts to distribute customer lists that contain credit card information.

When the policy analyzes a communication it creates a score based on its content. A communication must contain at least one instance of information indicative of a credit card such as an expiration date, CVV security number, a verification code, a credit card company name etc. and at least three valid credit card numbers. Typically, when a communication contains multiple credit card numbers, the surveilled user may have attempted to send out a customer list that contains sensitive client information.

Credit Report

Section § 603 of the Fair Credit Reporting Act defines a consumer report to be “Any written, oral, or other communication of an information be it a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for [Any purpose outlined in § 604 of this act]”. Section § 604 of the FCRA outlines the situations in which it is permissible to furnish a consumer report such as by court order (for child support purposes), “In accordance with the written instructions of the consumer to whom it relates”, “To a person which [the company] has reason to believe intends to use the information in connection with a credit transaction”, for employment, or for investment. Email surveillance provides a comprehensive solution that ensures the security of such information and prevents potential legal action, reputational damage, or potential regulatory ramifications.

The Credit Report policy protects against the distribution of consumer credit reports and credit information. This trigger scans for the major credit report providers (Experian, Equifax, Trans Union, etc.) as well as key words and language used in credit reports, such as bankruptcy judgment, credit score, foreclosure, etc.

The Credit Report trigger works by first analyzing a communication for information relating to one of the main consumer credit report providers such as Experian, Equifax, or Trans Union. Once one of these is identified the policy continues scanning the communication for information that is typically present on consumer credit reports such as “Creditor name”, “Account history”, or “Date of debt established”. When a customer defined threshold of matches is met, the trigger fires and flags the event for further review to determine the level of violation.

Customer Complaints: Response Prohibition

FINRA rule 4530(d) requires firms to report quarterly statistical and summary information regarding written customer complaints. FINRA uses the information to identify and initiate investigations of firms, branch offices and associated persona that may pose a risk, and for the timely identification of other regulatory matters in line with their goal of enhancing risk-based approaches to regulation, investor protection and market integrity. This rule also requires firms to promptly file with FINRA copies of specified criminal actions, civil complaints and non-FINRA arbitration claims. Customer satisfaction, then, is of paramount importance and any case of customer dissatisfaction needs to be noted. However this dissatisfaction occasionally stems, not from the product or service, but from the employee who provided them. Through email surveillance attempts to prevent a customer from filing a grievance can be caught before it results in more severe penalties.

Presenting the proper attitude and approach to your customer base is an imperative, and frequently that approach is measured through your dealings with customer dissatisfaction (customer complaints). The Response Prohibition trigger guards against an employee responding directly to a customer complaint by scanning for key words and phrases, such as apology/apologize, escalate to ..., take care of, repay, angry, etc., which identify a reply to a complaint.

The Customer Complaints: Response Prohibition trigger works by identifying language around attempts by a user to stop a customer from filing a formal complaint using phrases such as “This is good will gesture”, “I assure that I will fix this”, or “I’m sorry that you feel that way”. Once a customer determined amount of phrases such as these are identified, the trigger fires and flags the event for review to determine the level of violation.

Customer Complaints: Unprofessional Responses

FINRA rule 4530(d) requires firms to report quarterly statistical and summary information regarding written customer complaints. FINRA uses the information to identify and initiate investigations of firms, branch offices and associated persona that may pose a risk, and for the timely identification of other regulatory matters in line with their goal of enhancing risk-based approaches to regulation, investor protection and market integrity. This rule also requires firms to promptly file with FINRA copies of specified criminal actions, civil complaints and non-FINRA arbitration claims. While it does not specifically cover unprofessional responses, this rule covers the requirement to disclose customer complaints. Not only does responding unprofessionally to a complaint damage the general reputation of the company, but such responses could be a red flag to FINRA to launch an investigation into the matter. Using email surveillance, attempts to respond to a customer complaint in a negative, unprofessional, threatening, or otherwise aggressive manner, can be captured before resulting in potentially serious repercussions for the firm.

The Customer Complaints: Unprofessional Response policy captures communications that indicate a negative response to a complaint. The trigger scans for language in the appropriate context that may signal such an unprofessional response.

In detail, this trigger captures language around a complaint such as “You’re fault”, “Experienced a problem”, or “There was a mistake”. Once one of these pre-qualifiers is met establishing the possibility that there is a discussion about a complaint, the policy analyzes the communication for language that would indicate an “unprofessional response” such as “No one cares”, “Cut the Commission”, or “we were not at fault”. With this combination of phrases, the trigger fires and flags the event for review to determine the level of violation.

Customer Conditioning

Similar to Exclusivity, the Customer Conditioning policy focuses on language that indicates the intention to manipulate a customer or client to exclusively buy from the company or employee being monitored. The difference with this policy lies in the direction of the communication, which is to say who they are discussing it with. The Exclusivity policy focuses on the communications directed toward the customer or entity which the employee is attempting to coerce, or otherwise manipulate, into an exclusive relationship with their company. The Customer Conditioning policy focuses on communications between employees that show the intention of planning to do so. The focus of this policy is to prevent collusion between employees to manipulate a customer.

The Customer Conditioning policy works by identifying language indicative of collusion with another employee, in regards to monopolizing, or gaining exclusivity with a customer. Language such as “We’ll get them addicted”, “Depend on us”, “What option do they have”, “give them a discount too good to be true”, or “We know we have them” will flag the event as a potential violation. Once a predetermined threshold of matches is reached, the trigger fires and flags the event for review by an individual to determine the severity of the offense.

Customer Lists

The security of customer information is vital for several important reasons. Ensuring the security of client information allows the client to feel safe providing it, as well as maintaining a positive reputation in the business world. Typically, the information contained in a customer list is also protected by various regulations that were established to secure sensitive consumer information. Credit card number, Social Security numbers, account numbers, benefit enrollment information, individually identifiable health information, medical diagnostics etc. are all classified as information that is protected by federal regulations. In addition to regulatory requirements, there is also the need for general data security. Employees sending customer lists home, or to competitors, is a huge security risk that can result in a loss of customers and of revenue. However this type of information can be protected using an email surveillance solution.

The Customer Lists policy analyzes outgoing email for information that is common in customer lists such as phone numbers, addresses, and column names. The trigger further scans for multiple instances of the information indicating that it is part of a list.

The Customer Lists trigger identifies several key data elements that are typically found in client lists. The trigger first attempts to identify common column names such as “First Name’’, “Last Name”, “Client Name”, “Address”, or “Phone Number”, and then looks for specific instances of an email address, telephone number, addresses or address parts (including state codes, zip codes, UK postal codes). Once a customer defined threshold of events is reached the trigger fires and flags the event for review by a person who will determine the severity of the offense.

Customer Threats

The Customer Threats policy works to maintain a positive working relationship with clients. It is intended to monitor and capture communications from employees which may contain statements of an intention to take a hostile action on an individual, or entity, in retribution for something done or not done.

The Customer Threats policy works by identifying terms or language associated with taking hostile action such as “Cut you off”, “Kill the price stack”, “Stop services”, or “take steps to punish…” Once a predetermined threshold is breached, the policy flags the event for review by an individual.

Deceptive Language

Virtually every financial regulation outlines that providing false information is a punishable offense such as spreading rumors that may affect market integrity (FINRA Rule 2030, NASD Rule 435(5)). In addition, FINRA Rules 3110, 3010, and the SEC 17a 3-4 outline the requirements that all electronic communications relating to the business be monitored and retained. The Deceptive Language policy is a general "wide net" policy that provides a comprehensive solution intended to capture attempts of users to send communications that may include false or misleading information. Additionally, the policy is also intended to detect references that indicate inappropriate offline communications or relocating the conversation to a channel that is not monitored such as a personal phone.

The Deceptive Language trigger, as the name implies, looks for communications that may contain general deceptive language such as "Let's move this conversation offline", "Keep this between you and me", "You're sworn to secrecy", or "Don't send it in email, it'll be subject to scrutiny". As previously stated, this is a very broad and generalized policy and the language that is caught is not specific to just one specific subject. The language that this policy uses is often used in other policies to detect similar behavior around specific regulations (i.e. Dodd-Frank: End User Clearing). Typically, conversations that would contain such language are found in long email chains and chat rooms. Once a customer-determined amount of matches occur the trigger fires and flags the event for review.

Diagnosis Information

As outlined in §164.306 of the Health Insurance Portability and Accountability Act (HIPPA), covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce. This "Privacy Rule" outline is better known as Doctor-Patient Confidentiality, or Physician-Patient Privilege.

The Diagnosis Information policy is similar in concept to the Benefits Enrollment Information trigger. The Diagnosis Information trigger was also designed to meet HIPAA requirements and is critical in both medical and HR environments. This trigger scans for medical diagnoses, medical specialties, and the contextual use of each.

The trigger first looks for language that indicates a diagnosis or an indication that someone has a certain condition. Such language examples include “was diagnosed with…”, “He has come down with…”, or “The diagnosis is…”. The trigger then continues to search the communication for more specific language that indicates a specific medical condition, specific medical tests relating to the conditions, or potentially afflicted regions of the body. Typically, when disclosing diagnosis information, these three parts are mentioned with each other. Examples include “He had an MRI and we found that he had a brain aneurism”, “The test revealed an infection in the lungs”, or “After a blood test, patient was found to have a severe vitamin deficiency.” Once several instances of these keywords are identified the communication is flagged for review to determine if it is an actual violation.

Discriminations and Racism

Title VII of the Civil Rights Act of 1964 SEC. 2000e-2. [Section 703] (a) states “It shall be an unlawful employment practice for an employer - (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual’s race, color, religion, sex, or national origin; or (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual’s race, color, religion, sex, or national origin.”

This regulation prevents employers from discriminating while hiring or promoting individuals based on ethnic or cultural criteria, and helps to maintain a positive work environment where all employees feel safe. Though there are no direct laws concerning employee deportment or harassment, every company is concerned with the image that their representatives convey. This is true with their outward behavior as well as their written correspondence. The Discrimination and Racism policy monitors employee electronic communication and captures discretions before it can potentially develop into a more serious situation.

The Discrimination and Racism trigger works by scanning a communication for common words, phrases, racial slurs, or slang terms used in the colloquial vernacular that indicate racial insensitivity. The trigger includes specific slang terms which target individuals of Asian, African, Arabic, Hindi, Italian, Jewish, Hispanic, Caucasian, Native American, and Irish decent. Other phrases caught include “My boss is a racist”, “That comment offended me”, or “That was racially offensive”. Once a customer-determined threshold of matches is found, the trigger flags the email for review. Alternately, this trigger can block the communication from being sent.

Discrimination: Age

Title VII of the Civil Rights Act of 1964 SEC. 2000e-2. [Section 703] (a) states “It shall be an unlawful employment practice for an employer - (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual’s race, color, religion, sex, or national origin; or (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual’s race, color, religion, sex, or national origin.”

The Discrimination: Age policy is designed to capture employee behavior, in terms of demonstrating a biased against an individual based on age.

The Discrimination: Age policy works by searching a communication for language indicative of age discrimination such as “He’s too young/old for the job”, “force him/her to retire”, or “replacing the older/younger employees”. Once a predetermined threshold is breached, the event is flagged for review.

Discussion of Legal Proceedings

The UK Contempt of Court Act states "'the strict liability rule' means the rule of law whereby conduct may be treated as a contempt of court as tending to interfere with the course of justice in particular legal proceedings regardless of intent to do so. 2) Limitation of scope of strict liability. (1)The strict liability rule applies only in relation to publications, and for this purpose "publication" includes any speech, writing, [F1programme included in a cable programme service] or other communication in whatever form, which is addressed to the public at large or any section of the public." Similarly, EC 7-33 of the American Bar Association Model Rules of Professional Conduct states "A goal of our legal system is that each party shall have his case, criminal or civil, adjudicated by an impartial tribunal. The attainment of this goal may be defeated by dissemination of news or comments which tend to influence judge or jury. Such news or comments may prevent prospective jurors from being impartial at the outset of the trial and may also interfere with the obligation of jurors to base their verdict solely upon the evidence admitted in the trial. The release by a lawyer of out-of-court statements regarding an anticipated or pending trial may improperly affect the impartiality of the tribunal. For these reasons, standards for permissible and prohibited conduct of a lawyer with respect to trial publicity have been established."

Maintaining the confidentiality of legal proceedings is critical to any firm. The dissemination of news relating to the case, or the participants of the case, can have devastating effect on the case itself, changing the outcome or causing a mistrial. The Discussion of Legal Proceedings policy hedges this risk by providing a solution that monitors and captures the electronic communications of a surveilled user who mentions, refers to, or disseminates information about the legal specifics regarding a court proceeding.

The Discussion of Legal Proceedings trigger scans an email for the presence of language related to a legal process, action, or individual, which is to say the trigger looks for language such as "The Judge said…", "When he was getting indicted…", "Your testimony…", or "So and so is filing a lawsuit" rather than the formal and technical language of legal documents commonly called "Legalese".

Dodd-Frank: Disclosures

The Dodd-Frank Wall Street Reform and Consumer Protection Act was signed into law in July of 2010 and is a continuing work in progress today. There are many mentions about disclosure requirements in Dodd-Frank such as Title XV Section 1052 and 1503 and 1504. These sections outline the requirements for financial institutions that deal in mineral, mine operations, and natural gas commodities respectively, to provide form disclosures regarding the firm's activity in these areas. Section 404 covers disclosures around swap counterparties for special entities and broker dealers. Section 919 requires investor disclosures before the purchase of investment products and services, conflicts of interest disclosures, whistleblower disclosures. Section 932 covers disclosures for credit rating methodologies. Section 942 covers the disclosure and reporting requirements for asset-backed securities. There are numerous other disclosure requirements throughout the Dodd-Frank bill as one of the intentions of the act is to increase the transparency of financial instructions.

The Dodd-Frank: Disclosures policy is an all-encompassing, general blanket policy that monitors surveilled users' communicating the intention of omitting information from the required disclosure forms. The policy looks for a combination of deceptive language, quid pro quo language, and avoidance language indicating the intention to avoid disclosing certain information, or potentially lying about the information disclosed.

The Dodd-Frank: Disclosures trigger analyzes a communication for some type of deceptive or quid pro language such as "Do this and I will make it worth your while", "we can't tell anyone about this", "Do you think we could let this slide", or "Let do this under the radar". Upon uncovering an instance of this type of language, the trigger continues scanning the document for specific language relating to disclosures such as "mid-market mark", "Don't include this on the 8-k form", "We don't need to disclose this", or "We need to leave this off the MET". Once a customer-determined amount of matches occur the trigger fires and flags the event for review.

Dodd-Frank: End User Clearing

The Dodd-Frank Wall Street Reform and Consumer Protection Act was signed into law in July of 2010 and is a continuing work in progress today. Section 723 of the Dodd-Frank Act amended the Commodity Exchange Act (CEA) by adding Section 2(h)(1), which provides that "it shall be unlawful for any person to engage in a swap unless that person submits such swap for clearing to a derivatives clearing organization that is registered under [the CEA] or a derivatives clearing organization that is exempt from registration under [the CEA] if the swap is required to be cleared." The Dodd-Frank Act also added Section 2(h)(7) to the CEA, which provides that "the clearing requirement of Section 2(h)(1) shall not apply to a swap if one of the counterparties of the swap is not a financial entity, is using swaps to hedge or mitigate commercial risk and notifies the Commission in a manner set forth by the Commission, how it generally meets it financial obligations associated with entering into non-cleared swaps". The exception provided in Section 2(h)(7) is known as the "End User Exception".

The term "End-User" is defined as the true consumer of a product or service. The term is used to distinguish the person who will actually work with the goods or use the service from individuals who are involved in other stages of its development, production and distribution. The Dodd-Frank End User Clearing policy monitors for a combination of deceptive language, quid pro quo language, and avoidance language about clearing, and in turn prevents a person who is not considered an end user from attempting to illegally bypass the clearing step.

The Dodd-Frank End User Clearing trigger works by scanning a correspondence for some type of deceptive or quid pro language such as "Do this and I will make it worth your while", "we can't tell anyone about this", "Do you think we could let this slide", or "Let do this under the radar". Once an instance of this type of language is found, the trigger continues scanning the document for specific language relating to clearing such as "I'm not an end-user, but we can skip clearing on this one.", "We don't need to clear this" or some kind of trade or deal that would be required to be cleared such as "Trade rate is 5%", "swap on 3/5", or "3.5 bp on 3yr". Once a customer-determined amount of matches occur the trigger fires and the event is flagged for review.

Dodd-Frank: Influencing Clearing

The Dodd-Frank Wall Street Reform and Consumer Protection Act was signed into law in July of 2010 and is a continuing work in progress today. Section 726 states “In order to mitigate conflicts of interest, not later than 180 days after the date of enactment of the Wall Street Transparency and Accountability Act of 2010, the Commodity Futures Trading Commission shall adopt rules which may include numerical limits on the control of, or the voting rights with respect to, any derivatives clearing organization that clears swaps, or swap execution facility or board of trade designated as a contract market that posts swaps or makes swaps available for trading, by a bank holding company (as defined in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841)) with total consolidated assets of $50,000,000,000 or more, a nonbank financial company (as defined in section 102) supervised by the Board, an affiliate of such a bank holding company or nonbank financial company, a swap dealer, major swap participant, or associated person of a swap dealer or major swap participant.” As of 2012, this rule was finalized as part of CFTC Regulation 1.71. This rule outlines the restrictions on relationship with the clearing organization and states “Non-research personnel may not direct a research analyst's decision to publish a research report or direct the views and opinions in the report; Research analysts may not be under the supervision, control (including with respect to performance evaluation and compensation) of employees of the firm's business trading unit or clearing unit”

Influencing Clearing is the name given to the conflicts of interest rule outlined in Section 726 of the Dodd-Frank Act and defined in the new regulations regarding clearing. This section refers to the potential to send recommendations or bribes to any person or entity that is part of a derivatives clearing organization. The Dodd-Frank: Influencing Clearing policy scans for messages that contain recommendation language sent to an individual in clearing.

The Dodd-Frank: Influencing Clearing trigger works by first identifying a list of users (provided by the business) that are part of a derivatives clearing organization within the firm That list is loaded into the system and each user is identified according to their Clearing status. The policy then focuses on those users who are part of clearing (a “True” value) and will trigger based on language that indicates that another user is sending a recommendation. Once a recipient has been identified as being “In Clearing” the trigger continues to scan the communication for the presence of language indicative of a recommendation such as “I think you should…”, “In my opinion, it would be better to…”, “I recommend that you…”, or “My advice would be to…”. Once a customer-determined amount of matches occur the trigger fires and the event is flagged for review.

Dodd-Frank: Non-Associated Persons Discussing Swaps/Trades

The Dodd-Frank Wall Street Reform and Consumer Protection Act was signed into law in July of 2010 and is a continuing work in progress today. 17 CFR 23.22 of the Dodd-Frank bill states that "No swap dealer or major swap participant may permit a person who is subject to a statutory disqualification under section 8a(2) or 8a(3) of the Act to effect or be involved in effecting swaps on behalf of the swap dealer or major swap participant, if the swap dealer or major swap participant knows, or in the exercise of reasonable care should know, of the statutory disqualification; Provided, however, that the prohibition set forth in this paragraph (b) shall not apply to any person listed as a principal or registered as an associated person of a futures commission merchant, retail foreign exchange dealer, introducing broker, commodity pool operator, commodity trading adviser, or leverage transaction merchant, or any person registered as a floor broker or floor trader, notwithstanding that the person is subject to a disqualification from registration under section 8a(2) or 8a(3) of the Act".

An associated person is an individual who solicits orders, customers, or customer fund (or who supervises someone who does) on behalf of a Futures Commission Merchant, Retail Foreign Exchange Dealer, Introducing Brokers, Commodity Trading Advisor, or a Commodity Pool Organizer. Essentially an AP is anyone who is a salesperson for any of these categories of people or firms. The Dodd-Frank: Non-Associated Persons Discussing Swaps/Trades policy is intended to enforce this regulation by monitoring users designated as a non-associated person, and is designed to capture such activity before it occurs.

The Dodd-Frank: Non-Associated Persons Discussing Swaps/Trades policy first identifies a list of associated persons (provided by the customer and loaded into Orchestria) according to their AP status. The policy then focuses on those users who are not associated persons (a "False" value) and will trigger based on language that indicates that a swap is occurring, such as "Trade rate is 5%", "swap on 3/5", "3.5 bp on 3yr", "we need to amend the trade", or a reference to a type of swap such as a currency swap, plain vanilla swap, Interest Rate swap, equity index swap etc. Once a customer-determined amount of matches occur the trigger fires and the event is flagged for review.

Dodd-Frank: Non-Eligible Contract Participants

As defined in Section 1a(18) of the CEA The term “eligible commercial entity” means, with respect to an agreement, contract or transaction in a commodity, a financial institution, insurance company, a commodity pool that has total assets exceeding $5,000,000, a corporation or other entity with assets exceeding $10,000,000, an employee benefit plan subject to the Employee Retirement Income Security Act of 1974 that has assets exceeding $5,000,000, a government entity, a broker dealer that is subject to US regulations, a futures commission, an individual who has investments in excess of $10,000,000 or $5,000,000 if they enter into a contract in order to manage the risk associated with an asset owned by the individual, an investment adviser, or any other person that the commission determines to be eligible in light of the financial qualifications of the person. Parts of the Dodd-Frank act modify the existing Commodity Exchange Act (CEA). In Section 2(e) of the CEA it states that it is unlawful for a person that is not an eligible contract participant to enter into a swap, even if for hedging purposes, unless that swap is entered into over a board of trade that has been designated by the Commodity Futures Trading Commission as a contract market.

This policy monitors the communications to those considered by the rule as a non-eligible contract participant (based upon a list of Non-Eligible Contract Participants’ addresses provided by the customer), and identifies language that indicates that a trade is occurring. It also monitors the use of deceptive language concerning communicating over non-monitored channels and performing a non-compliant trade.

The Dodd-Frank: Non-Eligible Contract Participants trigger works by scanning a communication for the presence of legal entity names of the firm’s customers that are considered non-eligible contract participants (often in signatures of those associated with them). Once one of these entity names have been found, the trigger continues to scan for the presence of deceptive language such as “I don’t think we’re allow to do this”, “Not an ECP (eligible contract participant)”, “We don’t have to tell anyone” and language indicative of a trade or deal “Trade rate is 5%”, “swap on 3/5”, or “3.5 bp on 3yr”. Once a customer-determined amount of matches occur the trigger fires and the event is flagged for review.

Dodd-Frank: Political Contributions

The Political Contributions policy was designed to address the pay-to-play rules that are covered in 17 C.F.R. §23.451(b)(1) in the Dodd-Frank Wall Street Reform bill, that states "As a means reasonably designed to prevent fraud, no swap dealer shall offer to enter into or enter into a swap or a trading strategy involving a swap with a governmental Special Entity within two years after any contribution to an official of such governmental Special Entity was made by the swap dealer or by any covered associate of the swap dealer". This is an expansive policy covering not just Dodd-Frank but also § 130.6 of the International Traffic in Arms Regulations for Defense Contractors.

The design of this policy requires that some type of deceptive or quid pro quo language is present in the communication along with language, such as an email address or a title, identifying the recipient or sender as an elected official such as "Your Honor, Mr. Mayor, Mr. Vice-President etc.". The policy focuses on such language that would indicate trading a below-the-table deal for a donation to an elected official whether that donation is a gift, a sum of money, or an in-kind donation.

The language that is captured revolves around "this-for-that", "Vote no on this bill in exchange for a $2,000 contribution", "Don't worry, I can line your pockets Senator". For those keeping in the regulatory parameters of ITAR, language is added around avoiding the requirement to furnish certain political donation information to the Directorate of Defense Trade Controls. Under both definitions this policy captures attempts to give donations that are in excess of certain allowed dollar amount as described in the respective regulations.

When building the Political Contributions policy, all political offices were taken into consideration including state, city, and other locally elected officials, as well as the broad spectrum of politicians on the federal level including the House of Representatives, The Senate, State Governors (including territories overseen by the United States that have representation in government such as American Samoa, Puerto Rico, etc.), and the Executive Office. Three automated system definition updates run after each election to keep the list of elected politicians up to date for increased accuracy.

Dodd-Frank: Special Entities

A "special entity" is defined as a state or local municipalities, state or federal agencies, pension plans, governmental plans, and endowments. Section 1a(18) of the Dodd-Frank Wall Street Reform Bill refers to swap dealers' responsibilities with respect to special entities. A swap dealer that acts as an adviser to a special entity has a duty to act “in the best interests of” the special entity. These swap dealers, or MSPs, that perform a swap with a special entity must comply “with any duty” established by the swap dealer's regulator, the foremost being that they are “to have a reasonable basis to believe” that the special entity is advised by a qualified independent representative.

Because there is not a way to determine, using text alone, if a recommendation is “in the best interest” of the person it is sent to, The Dodd-Frank: Special Entities policy is designed to monitor communications that contains any kind of recommendation language. Events that trigger the policy to fire should be reviewed by an individual to make the determination if the content is a violation.

Designed to look for language concerning recommendations, suggestions, and giving advice, the Dodd-Frank: Special Entities trigger scans for phrases such as "I would recommend that we/you…", "Personally, if I were you, I would…", "I think you should…" and a list of legal entity names that fulfill the definition of a "special entity" as outlined above. The idea is that any recommendation going to a special entity will be monitored to ensure that the swap dealer, or major swap participant, is acting in the best interest of the special entity and that the communication is compliant with the new regulations.

Draft Documentation

The Draft Documentation policy captures the unauthorized, be it malicious or unintentional, distribution of unfinished materials. This policy was created to hedge against potential information breaches, as in sending out a confidential report before its made public, and to protect against the accidental distribution of draft copies to clients, in order to maintain a professional and polished appearance.

The Draft Documentation policy works by identifying language to indicate the version being distributed is not the final edit such as “Get back to me with any edits”, “Draft Copy”, “Kindly review the attached”, or “suggested changes/edits”. Once the predetermined threshold is met, the policy fired and flags the event for review by an individual.

Employee Evaluation Information

Every organization has a need to keep certain information confidential. HR is typically entrusted with maintaining sensitive employee information relating to employee and management issues. Such information includes Social Security numbers, performance reviews, workplace injury information, reference checks, health-related information, and pay levels. Legal issues, such as identity theft, data breach notifications and privacy laws, require employers to establish processes and procedures to secure and safeguard sensitive employee data and notify employees of any breach of this confidential information.

Data related to employee evaluations is generally considered to be private, so maintaining control of this information is a good business practice. The Employee Evaluation Information policy works in that regard by scanning for key words such as performance, review, assessment, appraisal, etc., as well as phrases (needs improvement, end of year review, self-assessment, the poor skills demonstrated, etc.) of the sort used in an employee evaluation.

The Employee Evaluation Information trigger works by first scanning a communication for keywords that indicate some kind of review such as "Rating", "Evaluation", or "Performance". Once the trigger identifies one of these pre-qualifiers, it will continue to scan for phrases such as "Areas in need of improvement", "Manager's feedback", or "S.M.A.R.T" (An acronym referring to an objectives setting guide). With this combination of phrases, the trigger fires and the event is flagged for review to determine the level of violation.

Exclusivity

The Exclusivity policy, designed to prevent aggressive handling of customers and avoid a potential of an Anti-Monopoly issue, searches for communications in which employees are attempting to force the customer into an exclusive business relationship by offering lower than normal prices or other unapproved benefits.

The Exclusivity policy works by identifying matches which might indicate that the employee being surveilled is making an offer which may not be within the guidelines of regulatory rules, or company standards. The policy looks for terms and phrases such as “Got them by the balls”, “Sell it to you way below cost”, “Make it so they don’t have an option”, or “Knock out the competitors (or the name of a competitor)”. After a predetermined threshold of matches is reached, the trigger fires and the event is queued for review by an individual to determine the severity of the violation.

Fair and Balanced Advice

FINRA Rule 2210 outlines the general standards for the content of advice that is disseminated. The rule states “All member communications must be based on principles of fair dealing and good faith, must be fair and balanced, and must provide a sound basis for evaluating the facts in regard to any particular security or type of security, industry, or service. No member may omit any material fact or qualification if the omission, in light of the context of the material presented, would cause the communications to be misleading.”

The Fair and Balanced Advice policy captures company communications where employees, who are legally allowed to give advice, could be giving misleading, or otherwise inaccurate advice to a client.

The Fair and Balanced Advice policy works by first identifying language involving various financial instruments or financial actions including funds, bonds, stocks, options, trades, calls, or puts. Once a match is found the policy continues to the next level, where it searches for language that is associated with potentially outlandish claims of “Better than the rest”, “Sky’s the limit”, or “Guaranteed outcomes”, in addition to “This will quadruple in value”, “the window of opportunity is closing”, or “won’t get another chance”. Once a predetermined threshold is met, the trigger fires and the event is flagged for review by an individual.

Fantasy Leagues

Fantasy sport leagues (also known as rotisserie or roto leagues) are a game where participants act as sport team managers, and pit their selected athletes against one another, tallying points based upon the athlete's performance. The Fantasy Leagues policy is intended to identify activities associated with fantasy league play by identifying various actions that can be performed in the game, professional team names, or various terms specifically associated with gameplay.

The Fantasy League trigger works by first analyzing a communication for the mentioning of various forms of sports fantasy leagues such as “Fantasy Football”, “Rotoworld Fantasy Baseball”, or “Roto Basketball”. Once any variation of these terms are identified, the trigger then continues to search for various terms such as actions associated with game play (“How’s your roster looking?”, “I want to make a player trade”, “Next week we go head-to-head”) or terms relating to professional team names and nicknames across multiple sports (“sixers”, “G-Men”, “Da Bears”, “Yanks”, “Manchester United” etc.). Once a customer-determined threshold of matches is met, the trigger fires and flags the event for review by an individual.

Financial Information – Balance Sheet

In financial accounting a balance sheet, also called a statement of financial position, is a summary of the financial state of a given business organization, including a sole proprietorship, a business partnership, a corporation, an LLC, or an LLP. A balance sheet is essentially a "snapshot of a company's financial condition" and of the three basic financial statements, it is the only statement which applies to a single point in time of a business' calendar year. Information such as this can potentially be used for the purposes of making trades or deals (with the explicit knowledge of a company's standing) for personal financial gain, known as insider information. For this reason, there is an urgency to ensure the security of such documents.

The Financial Information - Balance Sheet policy is one of four financial information policies that monitor, thereby ensuring, the security of financial non-public information. This financial information policy focuses specifically on the content and typical fields that are found on a balance sheet but does not require that an actual balance sheet be attached to the communication.

The Financial Information - Balance Sheet trigger looks for any and all information that can be present in a typical balance sheet. The policy first looks for common names of fields that are found on a balance sheet such as "assets", "Profit", "Inventory", or "Balance Sheet". Once any of these terms are found the trigger continues to search the email for specific information contained in a balance sheet such as "Gross profit/loss", "Accounts receivable", or "current assets". If a customer determined threshold of matches occurs the trigger fires and the event is flagged for review by an individual who will determine the level of violation. We recommend that a policy technician customizes the policy details to target the specific format of the balance sheet in use, and to increase the accuracy of this trigger.

Financial Information – Income Statement

A financial income statement, also known as a profit and loss account, profit and loss statement, revenue statement, statement of financial performance, earning statement, operating statement, or statement of operations, is one of the financial statements that show the company's revenue and expenses during a particular period. It indicates how the revenue, or top line, is transformed into the net income, or the bottom line. Information such as this can potentially be used for the purposes of making trades or deals, (with the explicit knowledge of a company's standing) for personal financial gain, known as insider information. For this reason, there is an urgency to ensure the security of such documents.

The Financial Information - Income Statement policy is one of four policies created to monitor the transmission of non-public financial information. This policy focuses on monitoring surveilled users attempting to distribute an income statement to an unauthorized individual or group of individuals. This policy is very general in terms of what it searches for so we recommend that a policy technician customize the policy details to target the policy toward the client specific income statement format, and to ensure the accuracy of triggered events.

The trigger first scans a communication for the presence of some keywords, such as “Income”, “Earnings”, “revenue”, or “cost of goods”, that might indicate the document, or information, is an income statement. Once one of these basic words is identified, the trigger continues to search for more specific language typically found on a statement of financial performance such as “Earnings Before Interest Tax”, “depreciation and amortization”, or monetary figures around “Operating Income”. When a customer defined threshold of matches is met, the trigger fires and the event is flagged for review by a person to determine the level of violation.

Financial Information – Projections

A financial projection is an estimate of future financial outcomes for a company using historical internal accounting and sales data, factors such as company plans, in addition to external market and economic indicators. Projections usually contain estimations of the firm's future sales, project variables such as expenses and assets, level of investment in current and fixed assets that is required to support the projected sales, and the firm's financial needs. Information such as this can potentially be used for the purposes of making trades or deals (with the explicit knowledge of a company's standing) for personal financial gain, known as insider information. For this reason, there is an urgency to ensure the security of such documents.

The Financial Information – Projections policy is one of four financial information policies that monitor, thereby ensuring the security of, financial non-public information. This policy monitors for language indicating future projections based on terms such as "projections", "plans" or "planning". This is a very basic policy and we recommend that a policy technician customize the policy to more accurately capture this sensitive information.

The trigger first scans a communication for the presence of some keywords that indicate the document, or information, is a projection such as "Business Plan", "Financial Planning Model", or "Financial Projection". Once one of these basic words is identified, the trigger continues to search for more specific language typically found on a statement of financial performance such as "Gross Profit", "Current Assets", or "Model Assumption". Based upon a customer defined threshold of matches, the trigger fires and the event is flagged for review by a person to determine the level of violation.

Foreign Language Detection

It is generally company policy that all communication takes place in English, as this is considered a universal standard when conducting business in English speaking countries. This is so that communications can be understood by those who do not speak another language and also for the purposes of regulatory electronic communication surveillance, as these systems typically only search for violations using English words and contextual phrases.

The Foreign Language Detection policy captures individuals speaking exclusively in a language that is not English, and also communications where a direct English translation is not provided.

The Foreign Language Detection policy depends on rules that are present in every language, regardless of origin. Adverbs, prepositions, interrogative/personal pronouns, and articles must be present for the communication to be understood by the person receiving it. In English, this would be similar to capturing any communication containing words like “the, and, in, at, of, it, he, she, we, I, who, what, why, how” etc. The foreign language detection policy looks for the linguistic equivalent of these in both the native and roman character sets of Mandarin Chinese, Cantonese, Spanish, Hindi, Russian, Arabic, Portuguese, Bengali, French, Malay, German, Japanese, Farsi, Urdu, Punjabi, Vietnamese, Javanese, Tamil, Korean, Turkish, Telugu, Marathi, Italian, Thai, Gujarati, Polish, and Hebrew. Since many of these words and languages are similar in root and form to English, the policy then takes the additional step of looking for these words being used in context with each other (“the” within 25 words or characters of “a, an, of”). Once a match is found the policy moves on to a list of negative indicators. This is a list of interrogative (Who, what, why) and personal (I, he, she) pronouns, prepositions (of, in, at), and articles (The, a, do). This is done in order to prevent the capture of communications that contain foreign language, with a direct English translation. Overall the policy will flag communications which contain a majority of foreign language in a ratio of 3:2.

Once these conditions are met, the policy captures the event so that it can be properly translated either by an individual or third party software. Once the message is properly translated it can be reviewed by an individual to determine the severity of the violation.

Forwarding Senior Management E-mail or Documents

In an enterprise environment it is not uncommon for emails from senior officials or executive management to contain sensitive information that, if circulated to unauthorized persons, could not only do significant damage to the firm in terms of regulatory violations, but could result in client mistrust and reputational damage, among other repercussions. Regulatory email surveillance provides a comprehensive measure to safeguard against such data loss and ensure that employees cannot distribute this information to unauthorized individuals.

The Forwarding Senior Management E-mail or Documents policy captures emails that have originated from an executive official. This is a very general policy and needs to be customized to the client's specific needs by a policy technician.

The Forwarding Senior Management E-mail or Documents trigger uses a list of the client's employees that are considered senior management. Using this list, the trigger scans an email for the "from:", "sent:", and "to:" fields, and searches for "FW" anywhere in the email. Once the name or email address of a person considered to be executive management is detected, the trigger fires and flags the event for review by an individual to determine the severity of the infraction.

Gambling Prohibition

The Gambling Prohibition policy captures the activity of employees engaging in non-work-related activity that can reduce productivity and company efficiency.

The Gambling Prohibition policy works by searching for language that indicates taking a bet, placing a bet, or other activities involved with gambling such as “Texas Hold-em”, “Put [amount of money] on the race/game”, “beat the odds”, or “chances of winning”. Once a predetermined threshold of matches occurs, the policy flags the event for review by an individual to determine the level of violation.

German Social Insurance Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The German Social Insurance Number policy captures the unauthorized distribution and dissemination of personally identifiable information, to ensure compliance with the various personally identifiable information regulations in many countries.

The German Social Insurance Number policy works by utilizing policy's pattern matching capabilities to identify a social insurance number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the German Social Insurance Number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of a German SIN. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Gifts and Entertainment

FINRA Rule 3220, regarding gifts and gratuities, states “No member or person associated with a member shall, directly or indirectly, give or permit to be given anything of value, including gratuities, in excess of one hundred dollars per individual per year to any person, principal, proprietor, employee, agent or representative of another person where such payment or gratuity is in relation to the business of the employer of the recipient of the payment or gratuity. A gift of any kind is considered a gratuity.” The regulation also states that “A separate record of all payments or gratuities in any amount known to the member, the employment agreement referred to in paragraph (b) and any employment compensation paid as a result thereof shall be retained by the member for the period specified by SEA Rule 17a-4”

Non-compliance with FINRA's rules, as well as your own corporate guidelines regarding gifts and entertainment, can lead to fines, loss of reputation and professional respect, and possibly legal issues. This policy looks for language that indicates an exchange of gifts, either given or accepted, by the surveilled user. The policy also focuses on entertainment such as sporting events and keywords from professional athletic teams (MLB, NFL, NBA, NHL), NASCAR and other sporting events, clubs, parties, shows, tournaments, concerts, theater, and various other activities that may be viewed as disproportional or inappropriate.

The Gifts and Entertainment trigger works by first identifying keywords or phrases such as "Doing each other a favor", "This cost me $800"(detects any amount of money), or "To show my appreciation". When the trigger identifies any one of these pre-qualifiers, it continues to search for language around giving gifts or types of gifts such as "I got us tickets to see the Red Sox (any baseball team will be caught), "Quid pro quo", "Can you get me tickets to the football game", or references to various inappropriate late night activities. Upon meeting a customer-defined threshold of matches, the trigger captures the event and flags it for review by a person who will determine if the event is egregious.

Guarantees and Assurances

FINRA Rule 2150(b), which replaced FINRA Rule 2330(e), "prohibits members and their associated person from guaranteeing a customer against loss in connection with any securities transaction or in any securities account of the customer. The reason for the prohibition is that such guarantees create the expectation that the customer is insulated from market risk intrinsic in securities ownership and may induce the customer to engage in a securities transaction that is not otherwise appropriate for the customer." The aforementioned rule also incorporates NYSE Rule 352(a), which states that "No member organization shall guarantee or in any way represent that it will guarantee any customer against loss in any account or on any transaction; and no member, principal executive, registered representative or officer shall guarantee any customer against loss in any customer account or on any customer transaction. The prohibitions in this paragraph extend to the payment, in whole or in part, or a debit balance"

Guarantees and assurances imply a set of financial promises that includes a set of associated risks, both financial and legal. This policy helps to ensure that only those authorized to provide guarantees and assurances do so, thereby reducing or eliminating this risk. Included in this policy's logic are key words and phrases, and detection for specific language that might imply a guarantee (It's like a blank check, this is going to be big bucks, you can buy/sell confidently, etc.)

The Guarantees and Assurances trigger works by first identifying a list of customer products (added into the system by a policy technician), or a general list of products or services that are offered by a financial institution such as "Stocks", "Options", or "Investments". These are known as pre-qualifiers, and once they are found in a communication the trigger continues to search for language that could indicate a guarantee such as "There will be little to no risk", "You have my guarantee that you won't lose anything", or "It's a risk-less deal". With this combination of phrases, the trigger fires and the event is flagged for review to determine the level of violation.

Harassment

Harassment such as racial discrimination is covered under Title VII of the Civil Rights Act of 1964 SEC. 2000e-2. [Section 703] (a) which states “It shall be an unlawful employment practice for an employer - (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual’s race, color, religion, sex, or national origin; or (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual’s race, color, religion, sex, or national origin.” Harassment such as age discrimination is covered under The Age Discrimination in Employment Act of 1967 SEC. 623. [Section 4] (a) which states “It shall be unlawful for an employer- (1) to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual’s age; (2) to limit, segregate, or classify his employees in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual’s age; or (3) to reduce the wage rate of any employee in order to comply with this chapter. (b) It shall be unlawful for an employment agency to fail or refuse to refer for employment, or other-wise to discriminate against, any individual because of such individual’s age, or to classify or refer for employment any individual on the basis of such individual’s age”. General workplace harassment, while not illegal, is often a violation of the standard code of ethical conduct at companies.

Though there are no “direct” laws concerning employee deportment or harassment, every company is concerned with the image that their representatives convey. This is true with their outward behavior as well as their written correspondence. Consequently, we have constructed a policy tailored to capture harassment attempts before they become a more severe issue. Using a lengthy list of graphic and slang words, and context checking to reduce false positives, this trigger scans for offensive or graphic language directly within the email, as well as any attachments.

The Harassment trigger works by analyzing a communication for “hazing” language or offensive language that is directed toward a specific individual. The trigger focuses on the explicate statement, or reference to, various acts of graphic or undesirable physical contact that is inherently sexual in nature. The trigger also looks for quid pro quo language for sexual contact, or general behavior that is designed to offend or annoy others. Once a customer-determined threshold of matches is found, the trigger flags the email for review, or the customer has the option to entirely block the communication from being sent.

Hong Kong Identity Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

Similar to the Chinese Identity Card Number policy, the Hong Kong Identity Card Number policy captures the unauthorized distribution and dissemination of Hong Kong's version of the Chinese identity card number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Hong Kong Identity Card Number policy works by first identifying the mention, or otherwise labeling, of the information in the communication ("HKID","Hong Kong Id card"). The policy also searches for the terms in their native Chinese Characters. Once a match has been identified, the policy uses a pattern matching definition to identify Hong Kong Identity Card Number in various formats. When both of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Inappropriate, Offensive, and Sexual Language

It is the responsibility of the employer to ensure that their employees are not exposed to language that they may deem inappropriate or offensive in the workplace. The means that the employer needs to take active steps to make sure that they have done everything possible to maintain an appropriate and non-hostile work environment. Language that is considered offensive is relative to the sensitivity of the listener; however there are groups of words and phrases that are always considered offensive. Additionally, the Federal Communications Commission has established a list of prohibited keywords that are considered a violation of federal law to broadcast at any time.

An employee conducting themselves professionally is an imperative. Though there are no direct laws concerning employee deportment or harassment, every company is concerned with the image that their representatives convey. This is true with their visible behavior as well as their written correspondence. Consequently, we have constructed a policy trigger tailored for inappropriate, offensive and sexual language. Using a lengthy list of graphic and slang words, and context checking to reduce false positives, this trigger scans for offensive language directly within the email, as well as any attachments.

The Inappropriate, Offensive, and Sexual Language trigger analyzes a communication for the presence of common ethnic colloquialisms, racial slurs, inappropriate or vulgar insults, or sexual terms, phrases, colloquialisms, and slang terms used in the local vernacular. Once a customer-determined threshold of matches is found, the trigger flags the email for review, or the customer has the option to entirely block the communication from being sent. Additionally, words that are on the FCC lists, and various permutations of those words where letters have been replaced with symbols or numbers, are considered definite matches and will always cause the policy to fire regardless of the surrounding content or customer defined threshold.

Indian Permanent Account Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Indian Permanent Account Number policy captures the unauthorized distribution and dissemination of India's version of the United Kingdom's National Insurance Number. This is designed to ensure the safety of the information that is entrusted to a company.

The Indian Permanent Account Number policy works by utilizing policy's pattern matching capabilities to identify a Permanent Account Number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Indian Permanent Account Number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of an Indian PAN. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Individually Identifiable Health Information (IIHI)

As outlined in §164.306 of the Health Insurance Portability and Accountability Act (HIPPA), covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce. This "Privacy Rule" outline is better known as Doctor-Patient Confidentiality, or Physician-Patient Privilege.

In keeping with regulations, the Individually Identifiable Health Information (IIHI) policy is intended to surveil users attempting to transmit information relating to an individual's health and information that can potentially reveal the identity of said individual. Specifically this trigger scans for names in association with addresses, phone number, birth dates, diseases, diagnoses, along with common medical terminology and symptoms.

The IIHI policy first looks to identify language signifying personal information. Such information may be in the form of a phone number, address, dates of birth, or in the case of spreadsheets, column titles such as "address", "First Name", "Last Name", "ZIP Code" etc. Once this information is found, the policy looks for language that more specifically targets medical information such as medical conditions, symptoms, admittance to a medical facility, prescription information, or the state/stage of certain conditions. With conditions met, the trigger fires and flags the event for review by a person to determine the severity of the infraction.

Indonesian Identity Card Number (Nomor Induk Kependudukan)

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Indonesian Identity Card Number (Nomor Induk Kependudukan) policy captures the unauthorized distribution and dissemination of personally identifiable information, to ensure compliance with the various PII regulations in many countries.

The Indonesian Identity Card Number (Nomor Induk Kependudukan) policy works by first identifying the mention, or otherwise labeling, of the information in the communication ("National ID"," Kartu Tanda Penduduk"), in both its English translation and in Indonesian, the native language of Indonesia. Once this condition is met, the policy uses a pattern matching definition to identify Indonesian Identity Card Numbers in various formats. When both of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Information Destruction Alert

There are numerous state and federal regulations regarding record retention and procedures for data disposal. SEC Rule 17a-4 Part 200 outlines the requirements by which records are to be kept, maintained, and to be made available for inquiry and inspection. The entire part outlines the guidelines for what information is to be kept and exactly for how long. NASD Rule 3010 (d)(3), regarding the regulatory requirement for supervision, states " Each member shall retain correspondence of registered representatives relating to its investment banking or securities business in accordance with Rule 3110. The names of the persons who prepared outgoing correspondence and who reviewed the correspondence shall be ascertainable from the retained records and the retained records shall be readily available to the Association, upon request."

Electronic information can be eliminated as easily as it was created, establishing a level of risk in regards to the uncontrolled destruction of retained data or documents. The Information Destruction Alert policy is designed to detect language indicative of a suggestion, or a direct command, to eliminate e-mail messages, files, or physical documents. The policy is intended to hedge against the risk associated with employees, whether by mistake or with malicious intent, deleting or physically destroying records.

The Information Destruction Alert trigger works by analyzing a communication for the presence of language indicative of the intent to purge, delete, or otherwise destroy information. The trigger looks for such phrases as "We need to delete everything we have on that", "Scrub the files", or "Wipe everything". The trigger also looks for potential indications of worry or urgency such as "Dump it all now!", "We have to cover this up", or "No one can find out, we have to purge everything immediately". When a customer-determined threshold of matches is reached, the trigger fires and flags the event for further review to determine the level of severity.

Information Security Label Control

It is common practice for a company to establish rules around the distribution of proprietary information. An information security label is a small disclosure that is applied to an email, attachment, or other form of electronic communication that indicates that the enclosed material cannot be shared, distributed, or divulged except to authorized individuals. The most common example of an information security label is the phrase "Do not disclose" or "Internal use only" somewhere in the body of the email or in the attachment itself.

The intent of the Information Security Label Control policy is to comply with company policy (or the specific request of the sender of the information) by preventing emails that are considered "Internal Use Only", "Secret", or "Strictly Confidential" from being sent, either outside of the firm, or to individuals who are not authorized to view the content.

The Information Security Label policy is meant for general protection from the unauthorized distribution of sensitive material and is considered a "blanket" policy to supplement existing policies that search for other specific content. The trigger searches for general terms and phrases that indicate the sender's request that the information disclosed here-in is not to be sent externally, or otherwise distributed without the specific consent or authorization from the original sender. Such phrases include "For your eyes only", "The message content here-in is protected", or "Not for external distribution". Once a customizable threshold of occurrences is met, the trigger fires and flags the event for review by a designated individual to determine the severity of the violation.

Inside Information: Front-Running/Trading Ahead

Front running is defined as the illegal practice of a stockbroker executing an order or a security for its own account while taking advantage of advance knowledge or pending orders from its customers. FINRA Rule 5270 states that "no member or person associated with a member shall cause to be executed an order to buy or sell a security or a related financial instrument when such member or person associated with a member causing such order to be executed has material, non-public market information concerning an imminent block transaction in that security, a related financial instrument or a security underlying the related financial instrument prior to the time information concerning the block transaction has been made publicly available or has otherwise become stale or obsolete" The rule was expanded to include "Related financial instruments" ("any option, derivative, security-based swap, or other financial instrument overlying a security, the value of which is materially related to, or otherwise acts as a substitute for, such security, as well as any contract that is the functional economic equivalent" as defined in Rule 5270(c)) in 2013.

Trading or dealing with inside information is in blatant disregard of other rules such as FINRA and SEC regulations (Sections 16(b) and 10(b)), SEC 17 CFR Parts 240, 243 and 249, and the UK Financial Services and Market Act, 2000, among many others. Therefore, it is imperative that we identify any correspondence exhibiting the intention to profit from inside information.

The Inside Information: Front-Running/Trading Ahead trigger works by first identifying a mention of one of the financial instruments and actions that are covered by the FINRA regulation such as the mention of a "Bond", "Selling shares", or "Options". When the trigger identifies any one of these pre-qualifiers, it continues to search for language around front running such as "Dump all of the stock", "You'll get a cut of the action", or a mention a transaction of ten thousand or more shares. Upon meeting a customer-defined threshold of matches, the trigger captures the event and flags it for review by a person who will determine if the event is egregious.

Inside Information: Non-Public Company Information Loss

Standard II: Integrity of Capital Markets states “Members and Candidates who possess material nonpublic information that could affect the value of an investment must not act or cause others to act on the information.” The regulation defines “material Information” as “if its disclosure would probably have an impact on the price of a security or if reasonable investors would want to know the information before making an investment decision. In other words, information is material if it would significantly alter the total mix of information currently available about a security in such a way that the price of the security would be affected.” Such information that is covered by this regulation “may include, but is not limited to, information on the following: earnings; mergers, acquisitions, tender offers, or joint ventures; changes in assets or asset quality; innovative products, processes, or discoveries (e.g., new product trials or research efforts); new licenses, patents, registered trademarks, or regulatory approval/rejection of a product; developments regarding customers or suppliers (e.g., the acquisition or loss of a contract); changes in management; change in auditor notification or the fact that the issuer may no longer rely on an auditor’s report or qualified opinion; events regarding the issuer’s securities (e.g., defaults on senior securities, calls of securities for redemption, repurchase plans, stock splits, changes in dividends, changes to the rights of security holders, and public or private sales of additional securities); bankruptcies; significant legal disputes; government reports of economic trends (employment, housing starts, currency information, etc.); orders for large trades before they are executed; and new or changing equity or debt ratings issued by a third-party (e.g. sell-side recommendations and credit ratings).”

The Inside Information: Non-Public Company Information Loss policy is intended to address the regulatory requirement to establish reasonably designed measures to restrict or limit the flow of information, which can be used by an individual to conduct unethical and unlawful trading. The focus of this policy is to hedge against the potentially unlawful distribution of information, relating to a company’s activities, which could affect the value of an investment or company, and thereby cause an individual to act on the aforementioned information.

The Inside Information: Non-Public Company Information Loss policy work by identifying language which could indicate a violation (a positive indicator). Phrases such as “The company will announce…”, “CEO will start Layoffs…”, “The result of the investigation into…”, “… entered into a merger agreement with…”, or “The CEO hinted towards his resignation”, all count toward the likelihood that the communication is a violation. In order to hedge against actual announcements, news articles, or public statements being flagged by the system, the policy will also search for the presence of words or phrases such as “Bloomberg News”, “Click here to unsubscribe”, or “Weekly (or other period of time) Newsletter”. These are considered negative indicators and will work to circumvent false positives. After all of these items have been identified, if the communication still breaches the threshold, it is flagged for review by an individual to determine the severity of the violation.

Inside Information: Non-Public Financial Information Loss

FINRA rule 5280 states “(a) No member shall establish, increase, decrease or liquidate an inventory position in a security or a derivative of such security based on non-public advance knowledge of the content or timing of a research report in that security.
(b) A member must establish, maintain and enforce policies and procedures reasonably designed to restrict or limit the information flow between research department personnel, or other persons with knowledge of the content or timing of a research report, and trading department personnel, so as to prevent trading department personnel from utilizing non-public advance knowledge of the issuance or content of a research report for the benefit of the member or any other person.” Disseminating non-public information relating to a company’s finances, can implicate not just the individual who conducted a financial transaction based on such information, but the source from which it was provided.

The Inside Information: Non-Public Financial Information Loss policy is intended to provide the aforementioned “policies and procedures reasonably designed to restrict or limit the information flow between research department personnel, or other persons with knowledge of the content or timing of a research report” by attempting to capture the unintentional or malicious distribution of non-public information, relating to a company’s financial standing.

The Inside Information: Non-Public Financial Information Loss policy works by identifying language which can be considered positive indicators of a financial report such as “Company’s expenses/expense report”, “Profit margins”, “Company growth”, “Loss of board members”, or “company cash flow”. Once a predetermined quantity of matches is identified, the event is flagged for review by an individual to determine the severity of the violation.

Inside Information: Rumors and Secrets

FINRA Rule 2030 defines a “rumor” as “a false or misleading statement or a statement without a reasonable basis” and the rule itself prohibits a member firm from “originating or circulating a rumor that ‘the member knows or has reasonable grounds for believing is false or misleading or would improperly influence the market price of a security’”. Rule 2030, established in 2009, replaces former FINRA Rule 6140(e). NYSE Rule 435(5) also prohibits the circulation of rumors of a sensational character “which might reasonably be expected to affect market conditions on the [New York Stock Exchange]”. FINRA Rule 2030 refers to rumors that may result in a change in the market price of securities, whereas NYSE Rule 435(5) covers rumors that may result in a change in the New York Stock Exchange listed prices.

The rumors and secrets flavor of the Insider Information policy is intended to provide a viable solution for preventing surveilled users from spreading such rumors, as described in FINRA Rule 2030 and NYSE 435(5), by looking for language that might indicate a rumor that could affect market conditions.

The Inside Information: Rumors and Secrets policy works by searching for rumor-indicative language such as “Have you heard about…”, “I hear they are going to announce something big”, or “Allegedly that deal is going to be approved” as well as deceptive language that could be indicative of a secret such as “Keep this hush-hush”, “Don’t tell anyone this.”, or “I’m telling you this in confidence”. Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Inside Information: Trading Ahead of Research

FINRA Rule 5280 combines Section 19(b)(1) of the Securities Exchange Act of 1934 and NASD Interpretive Material 2110-4 (IM 2110-4), both of which outline the regulations around trading ahead of research reports. IM 2110-4 states "that it is conduct inconsistent with just and equitable principles of trade for a member to establish or adjust an inventory position in an exchange-listed security traded over-the-counter or a derivative of such security in anticipation of the issuance of a research report on that security. The IM further recommends - but does not require - that firms establish policies and procedures to develop and implement effective internal controls to isolate specific information within research and other relevant departments so as to prevent the trading department from utilizing advance knowledge of the issuance of research reports." When this rule was adopted by FINRA Rule 5280, it changed three aspects of IM 2210-4. The first revision extends the application of the IM to cover inventory positions with respect to any security or derivative, regardless of whether the security is exchange listed or not. The second change states that the rule would apply only to circumstances where a member establishes or adjusts its inventory based on non-public advanced knowledge of the content or timing of a report. Lastly, the rule eliminates the option to establish internal controls to manage the flow of information between research and trading departments, and instead mandates that firms implement policies and procedures to restrict or limit the information being exchanged between the aforementioned departments.

Trading Ahead of Research involves establishing a position on a security in anticipation of a research report, the content of which can influence the price of a financial instrument. The Inside Information: Trading Ahead of Research policy scans for any language that indicates that the participants are discussing a position ahead of pending research. The policy also fulfills the new requirement in Rule 5280 that requires establishing "policies and procedures that are reasonably designed to restrict or limit" the information flow between individuals in trading and research departments.

The Inside Information: Trading Ahead of Research trigger works by identifying language typically used, as well as information contained, in research reports such as "Here is the completed research report", "This security is going to be downgraded", or deceptive hush-hush language such as "Promise that no one is going to find out", "This cannot go public", or "We should move this conversation to a private line". Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Intent to Resign

Professional courtesy dictates that your boss should be the first to learn of your intent to resign. While it's understandable, and even advisable, to seek the counsel of a trusted colleague while making the decision whether or not to leave your position, it's proper that the initial announcement should be made to your direct supervisor. In addition to this, preventing information from leaving the company is of paramount importance to the integrity, reputation, and the operation of a business. Employees actively expressing a desire to leave a firm, whether due to general dissatisfaction or otherwise, should be considered to be high risk because of the sensitive nature of the company information that they handle.

The idea of the Intent to Resign policy is to capture an employee's attempts to communicate with any other surveilled user regarding plans to leave the firm. The policy also looks for other resignation language that could convey job dissatisfaction, using the company's channels of communication to apply, or solicit a job or position from an outside source. This ensures that a resignation is handled delicately, confidentially, and professionally so as to not damage the reputation of the employee or the company, but also to assist in preventing the leakage of a company’s client information, or other sensitive company data, that the employee may attempt to take with them.

The Intent to Resign trigger works by analyzing a communication for language around quitting, seeking, or applying for another job. The trigger searches a communication for keywords and phrases such as online job sites like monster.com, careerbuilder.com, indeed.com, etc., indications of job dissatisfaction such as "I can't stand working under so and so anymore", "I really have to get out of this job", or "my job sucks", or attempts to apply to a job "I'm applying to this position", "I have an application in at another firm", or "I can provide references". Upon meeting a customer-defined threshold of matches, the trigger captures the event and flags it for review by a person who will determine if the event is egregious.

Internal Investigations

Internal investigations allow a company to review itself, ensuring that managers, supervisors, and employees are complying with the law as well as internal company policies and guidelines. In any sizable company, whether the situation is someone believing his or her rights are being disregarded, company policies are not being adhered to, or employees violating federal rules and regulations, it is the responsibility of the company to conduct a comprehensive, objective, and professional investigation regarding the matter. In order to ensure a fair and balanced process, details of the internal investigation, including subject, individuals, or intent, are considered classified and thus conversations relating to them are strictly prohibited. Communication surveillance hedges risk associated with the release of confidential and sensitive information before the appropriate time.

Due to the sensitive nature of internal investigations, The Internal Investigations policy was created with the intention to provide a comprehensive solution to prevent discussions concerning the existence, purpose, individuals, or results of a company specific internal investigation. The policy focuses on general language that is a combination of potential legal ramifications, secretive behavior, and inquiry.

The Internal Investigations trigger works by analyzing communications for such language that would be common when conducting an investigation such as speculations like "Who do you know that might be involved?" or "What do you think they are looking into?". The trigger will also look for language that indicates legal action such as "We may be facing a lawsuit", secretive language such as "If word of this gets out…", investigative language such as "What do you know about… and when did you know it?", or the acknowledgement of existence such as "We will be launching an investigation and looking into John Smith". Once a customer-determined threshold of matches is found, the trigger fires and flags the event for review.

Internal IT Support Documents

Protecting non-public information is a constant effort in large enterprise environments. In any company, often times there are rules and procedures governing the distribution of documents or other forms that can potentially contain information that should not be distributed. This includes documentation that can contain sensitive information regarding internal applications, network structure, or other systems outlined in detail in support documentation.

Working much like the Information Security Label Control trigger, the Internal IT Support Documents trigger looks for IT buzz words and phrases such as WAN, DMZ, packet switching, etc., and IT related NPI in attached documents.

The typical IT support document contains buzz words and key phrases, some of which may instruct an individual on how to resolve an issue with a particular piece of software, hardware, in a network environment, etc. This policy searches a communication for the presence of phrases like "MAC address", "Microsoft Windows Server", "Modem", or "Enterprise Network". A document that outlines instructions for troubleshooting IT related issues contains many instances of this language, and when the amount of matched language reaches a predetermined, customer defined, threshold the trigger fires and the flags event for review to determine the level of violation.

Investment Advice Prohibition

FINRA rule 1042 outlines the restrictions placed on Assistant Representatives stating that they "may not solicit transactions or new accounts on behalf of the member, render investment advice, make recommendations to customers regarding the appropriateness of securities transactions, or effect transactions in securities markets on behalf of the member. Persons registered in this category may not be registered concurrently in any other capacity." FINRA Rule 2210 states that "Retail communications or correspondence providing any testimonial concerning the investment advice or investment performance of a member or its products must prominently disclose the following: (i) The fact that the testimonial may not be representative of the experience of other customers. (ii) The fact that the testimonial is no guarantee of future performance or success. (iii) If more than $100 in value is paid for the testimonial, the fact that it is a paid testimonial." And FINRA Rule 2270 states that Day-Traders "providing investment advice for others or managing securities accounts for others may need to register as either an "Investment Adviser" under the Investment Advisers Act of 1940 or as a "Broker" or "Dealer" under the Securities Exchange Act of 1934. Such activities may also trigger state registration requirements."

It is the intent of every company to provide their customers with the best possible service, and to assist in achieving whatever goals the client may have. The Investment Advice Prohibition policy is designed to monitor communications from employees to ensure that only those individuals who are qualified, both in terms of legal standing and education, are administering the best possible, and most sound, advice in order to maintain a positive working relationship with the customer.

The Investment Advice Prohibition policy works by first identifying language relevant to giving advice. Phrases such as "It's my recommendation", "I'd suggest", or "You should consider", must be present before the policy continues searching a communication. Once a match is identified, the policy then looks for language indicating a type of investment, types of financial instruments, or types of financial transactions, such as "junk bond", "Non-rated debt", "CDO's", "Swap trade", "risk exposure", or "OTC Derivative ". Once a threshold of matches is met, the policy flags the event for review.

Irish Personal Public Service Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Irish Personal Public Service Number policy captures the unauthorized distribution and dissemination of Ireland's version of the United Kingdom's National Insurance Number. This is designed to ensure the safety of the information that is entrusted to a company.

The Irish Personal Public Service Number policy works by first identifying the mention, or otherwise labeling, of the information in a given communication ("PPSN", "Personal Public Service Number," etc.). Once a match is identified, the policy then searches for a personal public service number, which is done in two parts. First, the policy uses a pattern matching definition, which is tailored to identify the basic format of a Personal Public Service Number, and searches for any possible instances in a communication. If a match is identified, the policy then moves on to the second step, where the match found is validated using a base 23 Modulus check, the same basic mathematical principal used to verify Credit Card Numbers. Once all of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Italian National Identification Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Italian National Identification Number policy captures the unauthorized distribution and dissemination of Italy's version of the United States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Italian National Identification Number policy works by utilizing policy's pattern matching capabilities to identify a national identification number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Italian national identification number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of an Italian national ID Number. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Jokes

Created with the intention to provide a congenial work environment, the Jokes policy attempts to monitor and capture joke activity, the subject of which could be considered offensive, or otherwise inappropriate in the workplace.

The Jokes policy works by identifying positive language indicators that the individual is attempting to tell a joke such as “What do you get when”, “A [individual] walks into a bar”, or websites which contain such jokes. Once a predetermined threshold is reached the trigger fires, and queues the event for review by an individual to determine the severity of the violation.

Licensing Agreements

International Traffic In Arms Regulations § 124.1, regarding the manufacturing of license agreements and technical assistance agreements, states “The approval of the Office of Defense Trade Controls must be obtained before the defense services described in § 120.9(a) of this subchapter may be furnished. In order to obtain such approval, the U.S. person must submit a proposed agreement to the Office of Defense Trade Controls. Such agreements are generally characterized as either Manufacturing license agreements, technical assistance agreements, distribution agreements or off-shore procurement agreements, and may not enter into force without the prior written approval of the Office of Defense Trade Controls. Once approved, the defense services described in the agreements may generally be provided without further licensing in accordance with §§ 124.3 and 125.4(b)(2) of this subchapter. The requirements of this section apply whether or not technical data is to be disclosed or used in the performance of the defense services described in § 120.9(a) of this subchapter (e.g., all the information relied upon by the U.S. person in performing the defense service is in the public domain or is otherwise exempt from the licensing requirements of this subchapter pursuant to § 125.4 of this subchapter). This requirement also applies to the training of any foreign military forces, regular and irregular, in the use of defense articles. Technical assistance agreements must be submitted in such cases. In exceptional cases, The Office of Defense Trade Controls, upon written request, will consider approving the provision of defense services described in § 120.9(a) of this subchapter by granting a license under part 125 of this subchapter. Also, see § 126.8 of this subchapter for the requirements for prior approval of proposals relating to significant military equipment.” The term "intellectual property" is intangible property that is created in someone's mind such as art, literary works, music, inventions, designs, processes and trademarks. A license is a contractual right that allows the holder of the intellectual property to manage and protect it. When this information is property of a company or firm, ensuring the security of that information is of paramount importance. The US patent and Trademark Office and the US Copyright Office established laws and rules regarding the distribution of rights associated with intellectual property, such as a license. Additionally, Federal laws provide stiff civil and criminal penalties for pirating and other unauthorized use of intellectual properties.

The Licensing Agreements Policy is intended to prevent surveilled users from potentially violating any of the laws established regarding the unauthorized distribution of the rights to use intellectual properties whether unintentionally or maliciously. The policy attempts to capture emails and to alert reviewers of the potential violations before any legal infraction occurs.

The Licensing Agreements trigger scans a communication for the general presence of the word license, licenses, licensed. Once this general requirement is met, the trigger continues to scan for language indicative of a user providing licensing information such as "Grant of License", "Obtaining an exclusive license agreement", or "You may not modify the terms outlined in the license". Once a customer defined threshold of matches is reached the trigger fires and flags the event for review to determine the severity of the offense.

Macau Non-Permanent Resident Identity Card (BIRNP)

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

As opposed the Macau Permanent Resident Identity Card (BIRP), the Non-Permanent version of the policy captures the unauthorized distribution and dissemination of Macau's identity card number for individuals who are in the country on a visa, or otherwise do not permanently reside in the country.

The Macau Non-Permanent Resident Identity Card (BIRNP) policy works by utilizing policy's pattern matching capabilities to identify a Macau Non-Permanent Resident Identity Card number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Macau Non-Permanent Resident Identity Card Number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of a Macau NPRICN/BIRNP. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Macau Permanent Resident Identity Card (BIRP)

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Macau Permanent Resident Identity Card (BIRP) policy captures the unauthorized distribution and dissemination of Macau's version of the United States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Macau Permanent Resident Identity Card (BIRP) policy works by utilizing policy's pattern matching capabilities to identify a Macau Permanent Resident Identity Card number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Macau Permanent Resident Identity Card Number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of a Macau PRICN/BIRP. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Malaysian National Registration Identification Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Malaysian National Registration Identification Card Number policy captures the unauthorized distribution and dissemination of Malaysia's version of the United Kingdom's National Insurance Number. This is designed to ensure the safety of the information that is entrusted to a company.

The Malaysian National Registration Identification Card Number policy works by first identifying the mention, or otherwise labeling, of the information in the communication ("Kad Pengenalan", "NRIC"), in both its English translation and in the native language of Malaysia, Malay. Once this condition is met, the policy uses a pattern matching definition to identify Malaysian National Registration Identification Card Number in various formats. When both of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Medical Billings and Claims

In January of 2013, the Health Information Portability and Accountability act (HIPAA) was amended to include significant changes to the privacy, security, breach notification, and enforcement of the rules in regards to medical billing procedures. This rule expands the definition of a "business associated" to include an individual or entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity. This includes companies that code, bill and/or collect claims on behalf of a health care provider. The final rule also includes subcontractors that create, receive, maintain, or transmit protected health Information on behalf of a business associate that is covered under the HIPAA "business associate" definition. This new addition requires that any company that deals directly with medical billing or medical claims must comply with §164.306 of HIPAA laws that states "covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce."

The Medical Billings and Claims trigger was created with the original intent of data loss prevention; however with the addition of this new rule it is now a regulatory requirement for all persons who directly deal with medical billings. This trigger uses a combination of an NPI number (National Provider Identifier) with and without a Luhn check to identify any form as a medical claim. Once identified, the trigger delves further through the email or attachment for additional medical terms and context to confirm the nature of the event.

The NPI number is a unique identification number for covered heath care providers established as part of the HIPAA Simplification Standard. Covered health care providers and all health plans and health care clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10 position, intelligence-free numeric identifier with a check digit in the last position. This means that it is a simple ten digit number that does not contain any data identifying the client or health care provider. The last digit of the 10 digit number is a security feature to help detect potential keying errors or a fraudulent number. The NPI number is validated by putting 80840 before the entire number and verifying that this new 16 digit number adheres to the rules of the Luhn Algorithm.

This trigger scans a communication for the presence of a valid NPI number. Once that is detected, it continues searching for language confirming that it is an NPI number, or for billing language such as "Insurance company", "Co-pay", or language from forms such as the CMS 1500 (i.e. "Diagnosis or Nature of Illness or Injury”). With the NPI number and billing language identified, the policy fires and flags the event for review by a person who determines the severity of the infraction.

Medical History

As outlined in §164.306 of the Health Insurance Portability and Accountability Act (HIPPA), covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce. This "Privacy Rule" outline is better known as Doctor-Patient Confidentiality, or Physician-Patient Privilege.

As with the other medical triggers, the Medical History trigger conforms to the HIPAA requirements by analyzing a communication for the presence of medical information that may or may not pertain to an individual.

The Medical History trigger searches for a customer-determined minimum threshold of medical terminology that includes certain illness or ailments (i.e. amyotrophic lateral sclerosis (ALS), cirrhosis, and mononucleosis), medical symptoms (i.e. seizures, contractions, bleeding), prescription medication information (i.e. "50 mg", "amoxicillin", "Percodan"). Once this threshold is met, the trigger fires and captures the event, flagging it for review by a person who will determine the severity of the offense.

Medical Record Numbers

As outlined in §164.306 of the Health Insurance Portability and Accountability Act (HIPPA), covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce. This "Privacy Rule" outline is better known as Doctor-Patient Confidentiality, or Physician-Patient Privilege. Among the eighteen identifiers of PHI, as outlined in Section 1171 of Part C of Subtitle F of Public Law 104-191 (Federal Medical Privacy Standard), is medical record numbers.

In keeping with the compliance standards, the Medical Records Number Policy identifies electronic communications that may contain a medical record number. This trigger scans for record number strings, select key words, and contextual usage of those words that indicate the event concerns medical record numbers.

Unlike other personally identifiable information there is not a standardized or specifically defined pattern for medical record numbers. Typically, an organization will create their own standardized pattern for medical record numbers and because of this the "out of the box" version of the policy simply looks for any number five to ten digits in length, along with other information detailing that it is a medical record number (i.e. "Medical Number", "Patients ID number", etc.). Before introducing this policy to a production environment, we recommend that a policy technician create a pattern matching definition to accurately identify the standard convention that the company uses. Once an event triggers the policy to fire, it is flagged for review by a designated individual to determine the severity level of the violation.

Medical Record Numbers – Threshold

As outlined in §164.306 of the Health Insurance Portability and Accountability Act (HIPPA), covered entities and businesses associated must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate created, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the aforementioned regulation; and ensure compliance with this subpart by its workforce. This "Privacy Rule" outline is better known as Doctor-Patient Confidentiality, or Physician-Patient Privilege. Among the eighteen identifiers of PHI, as outlined in Section 1171 of Part C of Subtitle F of Public Law 104-191 (Federal Medical Privacy Standard), is medical record numbers.

In keeping with the compliance standards, the Medical Records Number – Threshold Policy identifies electronic communications that may contain a certain number (or threshold) of medical record numbers. This trigger scans for record number strings, select key words, and contextual usage of those words that indicate the event concerns medical record numbers.

Unlike other personally identifiable information there is no standardized or specifically defined pattern for medical record numbers. Typically, an organization will create their own standardized pattern for medical record numbers. Consequently, the "out of the box" version of the policy simply looks for any number five to ten digits in length along with other information detailing that it is a medical record number (i.e. "Medical Number", "Patients ID number"). The threshold version of this policy identifies events containing a specific amount of medical record numbers which indicate a list. Before introducing this policy to a production environment, we recommend that a policy technician create a pattern matching definition to accurately identify the standard convention that the company uses. Once an event triggers the policy to fire, it is flagged for review by a designated individual to determine the severity level of the violation.

Mergers and Acquisitions

FINRA rule 5280 states “(a) No member shall establish, increase, decrease or liquidate an inventory position in a security or a derivative of such security based on non-public advance knowledge of the content or timing of a research report in that security.
(b) A member must establish, maintain and enforce policies and procedures reasonably designed to restrict or limit the information flow between research department personnel, or other persons with knowledge of the content or timing of a research report, and trading department personnel, so as to prevent trading department personnel from utilizing non-public advance knowledge of the issuance or content of a research report for the benefit of the member or any other person.” FINRA Rule 2720 outlines the rules around participations in public offerings.

The Mergers and Acquisitions policy captures the activity of an individual discussing such a transaction where the information could be used to trade ahead of public knowledge, or an individual attempting to conduct a transaction which could violate the rules of public offerings set forth in Rule 2720.

The Mergers and Acquisitions policy works by identifying language which can be considered a positive indicator of a discussion relating to mergers and acquisitions, such as “Escrow share register”, “No-shop provision”, “aggregate exercise amount”, or “Investor rights agreement”. Once a predetermined threshold of matches is identified, the policy triggers and queues the event for review by an individual to determine the severity of the violation.

Network Security Threats

A company's security is integral to their reputation, and is mandated as part of regulations stating that a company must "establish, maintain and enforce policies and procedures reasonably designed to restrict or limit the information flow". The prevention of Network attacks is therefore paramount to a company and the integrity of the client specific, or personally identifiable, information.

The Network Security Threats policy captures discussions involving breaching a network through various technical methods, tools, or utilities.

The Network Security Threats policy works by identifying methods by which individuals can gain unauthorized access to a network system. Mention of tools such as "Aircrack", "packet sniffers/sniffing", or "Kismet" is an immediate flag in the system and triggers the policy for review by an individual to determine the severity of the violation.

Office Relationships: Romantic

Companies typically have HR regulations governing intra-office relationships, with the intention of separating the work place from personal business, preventing hostile work environments, or avoid making co-workers uncomfortable. In addition to providing a comfortable work environment, these guidelines also help to prevent situations involving favoritism or unfair treatment of employees. The Office Relationships: Romantic policy is designed to capture such employee behavior, and to ensure that office romances abide the rules set forth by Human Resources.

The Office Relationships: Romantic policy works by identifying language indicating a relationship may exist outside of the work place, such as terms of endearment (“Hunny”, “Babe”, “Sweetheart” etc.), expressions of affection (XOXO, indications of a physical relationship), or attempts to generate such a romantic relationship (“Let’s get dinner”, “We should go out sometime”). Once a predetermined threshold is reached the trigger fires, and queues the event for review by an individual to determine the severity of the violation.

Outside Business Activity/Directorships/Employment

In accordance with FINRA Rule 3270, "No registered person may be an employee, independent contractor, sole proprietor, officer, director or partner of another person, or be compensated, or have the reasonable expectation of compensation, from any other person as a result of any business activity outside the scope of the relationship with his or her member firm, unless he or she has provided prior written notice to the member, in such form as specified by the member. Passive investments and activities subject to the requirements of NASD Rule 3040 shall be exempted from this requirement." This regulation essentially outlines the requirement that all registered persons employed at a financial institution are required to disclose all outside business activity to the member institution. The reason for this disclosure is to ensure that any outside business activities do not present a conflict of interest, in regards to the employee's position or power to make decisions.

While any outside business activity needs to be disclosed and approved, it is generally company policy for employees to not conduct said business using company resources or channels of communication. The Outside Business Activity/Directorships/Employment policy is intended to monitor, and to prevent, employees conducting their outside business using company email, IM, or other surveilled methods of communication.

The Outside Business Activity/Directorships/Employment trigger works by analyzing communications containing language indicative of promoting a personal venture such as "I have my irons in the fire" or "You can get in on the ground floor of this". The trigger also looks for language around planning to start a business such as "We should go into business together" or "I 'm going to open my own eBay story". Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Pakistan National Identity Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Pakistan National Identity Card Number policy captures the unauthorized distribution and dissemination of personally identifiable information, to ensure compliance with the various PII regulations in various countries

The Pakistan National Identity Card Number policy works by first identifying the mention, or otherwise labeling of the information in the communication ("National Identity Card"," قومی شناختی کارڈ "), in both its English translation and in the native language of Pakistan, Urdu. Once this condition is met, the policy uses a pattern matching definition to identify Pakistan National Identity Card Numbers in various formats. When both of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Parking and Wash Trades

Wash trading is defined as “the process of buying shares of a company through one broker while selling shares through a different broker. Wash trading can also make a stock's volume appear to have a lot of activity resulting from the repeated buying and selling done by an individual or firm when, in fact, the shares have never changed owners.” Parking is defined as “A form of kiting shares that a brokerage commits by moving long positions in unrelated accounts to cover short positions that are improperly settled according to SEC regulations.” Both of these stock market practices are banned by NYSE rules and regulations.

The Parking and Wash Trades policy provides a comprehensive solution to identify users attempting to commit such acts. In accordance with the Williams Act amendments to the SEC Act (15 U.S.C.A. § 78a et seq.) regarding full disclosure of tender offers, the Parking and Wash Trading trigger monitors for cash trade offers.

The Parking and Wash Trades trigger works by first looking for language that indicates the individual is discussing some type of trade such as “Bonds”, “Shares”, “Stocks”, or “Security or Securities”. Once the trigger matches one of these pre-qualifiers it continues to scan the communication for the presence of parking and wash trading language such as “We can replace the shares quickly”, “Game the system”, “Buy it back after 30 days”, or “We need to hide the trade”. Once a customer-determined threshold of matches is found, the trigger flags the email for further review.

Patent Applications

Intellectual Property Regulations (37 C.F.R.) §1.14 (a)(1), regarding confidentiality of patent application information, states “Patent applications that have not been published under 35 U.S.C. 122(b) are generally preserved in confidence pursuant to 35 U.S.C. 122(a). Information concerning the filing, pendency, or subject matter of an application for patent, including status information, and access to the application, will only be given to the public as set forth in § 1.11 or in this section. (1) Records associated with patent applications may be available in the following situations: (i) Patented applications and statutory invention registrations (ii) Published abandoned applications (iii) Published pending applications (iv) Unpublished abandoned applications (including provisional applications) that are identified or relied upon (vi) Unpublished pending applications (including provisional applications) that are incorporated by reference or otherwise identified (vii) When a petition for access or a power to inspect is required”

Protecting intellectual property is imperative to any business, and allowing that information to leave the company may be in violation of your company's confidentiality policy, as well as an outright theft. With this policy we aim to detect non-public patent applications being discussed or disclosed in email.

The Patent Applications trigger will start to scan a given communication as long as the word patent or patents is present. Once this is confirmed the trigger will continue to analyze the communication for language that is typically found in a patent application such as a "First Named Inventor", "Title of Invention", or various permutations that are indicative of a PTO number. Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Potential Ethical Issues

Although we all have an understanding of ethics, it can be difficult to explain what it is in simple terms. In a sense, every regulation is designed to promote ethical behavior. Specifically, 29 C.F.R. 0.735 outlines the employee ethical conduct standard for government employees. In the financial industry, FINRA Rule 2111 regarding suitability states “Implicit in all member and associated person relationships with customers and others is the fundamental responsibility for fair dealing. Sales efforts must therefore be undertaken only on a basis that can be judged as being within the ethical standards of FINRA's rules, with particular emphasis on the requirement to deal fairly with the public. The suitability rule is fundamental to fair dealing and is intended to promote ethical sales practices and high standards of professional conduct.” FINRA rule 2111 outlines the requirement that an investment strategy meets the objectives and means of an investor, or is suitable for the investor.

The Potential Ethical Issues policy is an all-encompassing, general blanket policy that monitors surveilled users’ electronic communications for concerns about potential ethical matters. The policy looks for general, non-specific, language that indicates that the user is communicating a concern or attempting to perform an action that is a potential ethical violation to either a federal regulation, or a company policy.

The Potential Ethical Issues trigger scans a communication for non-specific deceptive language indicating a potential breach in ethical conduct such as “Keep this on the down low”, “They are getting cheated”, or “This can never be made public”, or language expressing concern such as “Guys, I don’t think we should be doing this”, “I have to bring this to so and so’s attention”, or “This doesn’t seem very kosher”. Once a customer-determined threshold of matches is identified, the trigger fires and flags the event for review to determine the level of violation.

Potential Legal Issues

Any type of business, even those with one or only a few employees, must follow state and federal regulations in terms of labor, financial, tax, and discrimination laws, standards, and regulations etc. If a product, service or an employee or agent harm a customer or member of the public, a company might be liable for damages. When an employer or employees act unethically, even if the law is not technically broken, this can still result in damage to the firm. If the public believes a firm discriminates against customers or employees, tries to skirt various laws, doesn't honor certain agreements, or generally acts unethically, these notions can result in reputational damage. Creating detailed company policies and procedure guidelines, and monitoring the behavior of employees through their electronic communications, can provide a substantial decrease in risk for the company.

Questions are often circulated internally about the legality of a particular action or business practice without informing a legal representative until the problem has been made public or resulted in harm. The Potential Legal Issues policy is intended to monitor surveilled users for language that is indicative of an employee mentioning, questioning, or expressing concern regarding the potential legal ramifications of an action.

The Potential Legal Issues trigger is designed to look for a combination of deceptive language, with or with some legal terminology, as well as secretive language such as "I don't know how legal something like that would be", "I'm pretty sure this violates a ton of laws", "I'm pretty sure that's illegal in every country and seriously frowned upon in Amsterdam", or deceptive/secretive language such as "let's keep this our little secret", "We can't let anyone find out", or "We need to keep this between us". Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Pricing List

Corporate policy typically mandates that non-public information such as pricing list, financial data or other forms of pricing or sales data cannot be distributed outside of the firm. Pricing lists also fall under the Standard II: Integrity of Capital Markets definition for non-public information. The regulation states “Members and Candidates who possess material nonpublic information that could affect the value of an investment must not act or cause others to act on the information.” The regulation defines “material Information” as “if its disclosure would probably have an impact on the price of a security or if reasonable investors would want to know the information before making an investment decision. In other words, information is material if it would significantly alter the total mix of information currently available about a security in such a way that the price of the security would be affected.” Such information that is covered by this regulation “may include, but is not limited to, information on the following: earnings; mergers, acquisitions, tender offers, or joint ventures; changes in assets or asset quality; innovative products, processes, or discoveries (e.g., new product trials or research efforts); new licenses, patents, registered trademarks, or regulatory approval/rejection of a product; developments regarding customers or suppliers (e.g., the acquisition or loss of a contract); changes in management; change in auditor notification or the fact that the issuer may no longer rely on an auditor’s report or qualified opinion; events regarding the issuer’s securities (e.g., defaults on senior securities, calls of securities for redemption, repurchase plans, stock splits, changes in dividends, changes to the rights of security holders, and public or private sales of additional securities); bankruptcies; significant legal disputes; government reports of economic trends (employment, housing starts, currency information, etc.); orders for large trades before they are executed; and new or changing equity or debt ratings issued by a third-party (e.g. sell-side recommendations and credit ratings).”

Due to the fact that the prices of a company’s products and services are considered non-public, the Pricing List policy captures various types of pricing lists. To that end, the Pricing List policy looks for telltale signs of price list information including currency names/types, and other product pricing nomenclature, all in an appropriate/expected sequence.

The Pricing List trigger works by analyzing a communication for specific indicators that show that the contents include a pricing list. It does this is by searching for indicators such as the word “Pricing” within 100 words or numbers of a type of currency such as yen, pounds, or dollars. Another pattern that the trigger searches for is for words such as “Lists”, “Unit”, “Inventory”, or “Net” in the proximity of a number or type of currency. In it’s out of the box form, this policy is extremely broad and requires a level of refinement to tailor the policy to the environment and intent of the client. Once a customer-determined threshold of matches occurs, the trigger captures the event and places it in a queue to be reviewed.

Product and Design Specifications

The Product and Design Specifications policy is a DLP (Data Loss Prevention) policy designed to prevent the unauthorized distribution of confidential company information as it pertains to new, unreleased products and product designs that are currently in development.

The Product and Design Specifications policy works by first identifying a mention of a design, functional specification, or language indicative of a configuration and/or layout of a product. Once one of these is identified, the policy looks for additional positive indicators and sensitive material such as “Drawing number”, “blueprints”, “Product dimensions”, “above/below diagram”, to name a few. When a predetermined threshold of matches is reached, the trigger fires and flags the event for review by an individual to determine the level of offense.

Project Information

In any environment where there are major business projects, many of them can be considered part of the non-public information (NPI) domain. Information regarding activities pertaining to company restructuring, software releases, plans to take on or to drop a client, etc., should not be divulged until it is considered advantageous to the company. Any leak could be devastating to not only the project, but the company itself in terms of reputational damage, company devaluation, or in some cases, regulatory penalties. Email surveillance provides comprehensive preventative measures against such information leakage and is a valuable tool in data loss prevention.

The Project Information policy is yet another trigger designed to protect non-public information regarding project planning and status information, project tracking, project codes, and management tools. This is a general policy meant to capture only the basic language associated with projects. We recommend that a policy technician customize the policy details to target language around a specific project, or adapt the policy to capture the local vernacular.

As with all policies, this trigger can be directed to focus on communications going outbound, coming inbound, or being sent to individuals in the firm, and ensure that information is not being sent to any individual who is not authorized to view it. The trigger, in its most basic form, looks for keywords or phrases indicative of a project discussion such as "Here are the details on project apple", "The status report", "and scope statement", or "He is in charge of resource management for this project". Once a customer determined amount of matches have been confirmed, the trigger fires and flags the event for review by a person to determine the severity of the violation.

Proprietary Software Code

In any environment there is a risk of data loss of in-house source code. This policy trigger scans emails for unique identifiers that indicate the email contains source code. Using contextual scanning and matching for keywords and symbols (such as ARGV, ParamArray, ifdef, and {, |, and ~, among many others), the Proprietary Software Code trigger looks to intercept any source code and source code snippets.

SQL language revolves heavily around actual words rather than symbols or variable definitions. Common statement such as SELECT, INSERT, UPDATE, CREATE, TRUNCATE, DROP, DELETE are all pattern matched to reduce false positives. This results in actual SQL statements such as “Select * FROM EmployeeInformation” firing the trigger rather than portions of everyday conversation.

For C++ the trigger scans for keywords associated with the language such as #Include, #Endif, typedef, as well as patterns associated with a semi-colon to end a line. The pattern matching definitions differentiate between the grammatical use of a semi-colon and the code use, for example “int main (int argc, char *argv[]);” versus “More than 900 million people still lacked access to clean drinking water in 2010; and 2.6 billion did not have adequate sanitation”.

Python is a commonly used language in enterprise applications and the trigger focuses on the keywords that are commonly used, such as DIS.DIS, FH.WRITE, FH.CLOSE, RE.MATCH, and MATCHOBJ along with pattern matching strings that identify Python code.

The design of this policy trigger allows for not just the specific targeted languages but addresses many programming languages that contain similar indicators. Consequently, the policy triggers on more than just the specified languages, including C, C#, Perl, and all ANSI standard SQL queries regardless of platform (MSSQL, Oracle, MySQL, Postrge, Sybase, etc.).

Sales Information

The release of confidential, non-public information can be devastating to the reputation and value of a company and, in some cases, can result in various regulatory penalties. In any enterprise level company, the security of information pertaining to sales is of vital importance due to the potentially sensitive nature of the transaction. Email surveillance provides a comprehensive preventative solution to stop such information leakage before it becomes an issue and is integral in general data loss prevention.

The Sales Information policy is a generic policy intended to capture the attempts of users to distribute information relating to the logistics, commission and discount rates, client lists, fees and fee structure, pricing, etc. of a sale.

Due to the extremely basic nature of the "out-of-the-box" policy parameters, we recommend that a policy technician create a more comprehensive policy that accurately captures the required information. The basic trigger searches for words and key phrases that indicate information regarding a sale or transaction is being sent such as "retail pricing", "services agreements", or "SOW (statement of work)". Once a client determined threshold of matches is achieved, the event is captured and flagged for review by a designated individual to determine the level of violation.

Singapore National Registration Identity Card

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Singapore National Registration Identity Card policy captures the unauthorized distribution and dissemination of Singapore's version of the United States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Singapore National Registration Identity policy works by utilizing policy's pattern matching capabilities to identify a Singapore National Registration Identity number in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Singapore National Registration Identity number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of a Singapore NRI. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Social Security Number

In accordance with the Code of Federal Regulations § 422.103, the Social Security Administration (SSA) maintains a record of the earnings reported for each individual who is assigned a social security number. The Fair and Accurate Transactions Act (FACTA) requires financial institutions and creditors that maintain covered accounts for their customers to create a written program to detect, prevent, and mitigate identity theft. Further, the Federal Trade Commission has published a legal rule called the Red Flags Rule (most recently amended in the Dodd-Frank: Wall Street Reform and Consumer Protection Act) that establishes a program with four basic elements to help prevent potential identity theft.

The Social Security Number policy looks for the presence of a valid social security number and uses the assigning convention, as created by the SSA, to determine the authenticity of a social security number. When an event triggers the policy that event is flagged for further review.

A social security number is valid if it is a nine-digit number in the format “AAA-GG-SSSS”. The first 3 digit set of numbers are determined by an individual’s geographic location. The middle segment is the group number which can range from 01-99. The final segment is known as the serial number which can range from 0001-9999 and is assigned randomly to an individual.

This trigger requires that at least one formatted or unformatted social security number is present along with confirmation that the number is a social security number. For example: “SSN: 123-45-6789” does not cause the trigger to fire on the event as the number is not a valid social security number in accordance with the SSA assigning convention. A communication containing language such as “987-65-4320 is her social security number” will cause the policy to capture the event at which point it is flagged for review by an individual to determine if the event is an true positive.

Social Security Number – Threshold

In accordance with the Code of Federal Regulations § 422.103, the Social Security Administration (SSA) maintains a record of the earnings reported for each individual who is assigned a social security number. The Fair and Accurate Transactions Act (FACTA) requires financial institutions and creditors that maintain covered accounts for their customers to create a written program to detect, prevent, and mitigate identity theft. Further, the Federal Trade Commission has published a legal rule called the Red Flags Rule (most recently amended in the Dodd-Frank: Wall Street Reform and Consumer Protection Act) that establishes a program with four basic elements to help prevent potential identity theft.

The Social Security Number – Threshold policy looks for multiple instances of valid social security numbers by using the assigning convention, as created by the SSA, to determine the authenticity of a social security number. When an event triggers the policy that event is flagged for review by a designated person to determine whether the communication contains a genuine violation.

A social security number is valid if it is a nine-digit number in the format “AAA-GG-SSSS”. The first 3 digit set of numbers are determined by an individual’s geographic location. The middle segment is the group number which can range from 01-99. The final segment is known as the serial number which can range from 0001-9999 and is assigned randomly to an individual.

This trigger uses the same parameters as the Social Security Number policy to determine the presence of a valid social security number. However, in order for this policy to trigger there needs to be more than one instance of a social security number, or a threshold amount. The intent here is to capture attempts to distribute potential customer lists that contain sensitive information.

Social Security Number with Additional PII (Personally Identifiable Information)

In accordance with the Code of Federal Regulations § 422.103, the Social Security Administration (SSA) maintains a record of the earnings reported for each individual who is assigned a social security number. The Fair and Accurate Transactions Act (FACTA) requires financial institutions and creditors that maintain covered accounts for their customers to create a written program to detect, prevent, and mitigate identity theft. Further, the Federal Trade Commission has published a legal rule called the Red Flags Rule (most recently amended in the Dodd-Frank: Wall Street Reform and Consumer Protection Act) that establishes a program with four basic elements to help prevent potential identity theft.

The Social Security Number with Additional PII policy looks for any instance of a valid social security number by using the assigning convention, as created by the SSA, to determine the authenticity of a social security number. In addition, this policy looks for any information, such as address, phone number, date of birth etc. that can identify an individual. When an event triggers the policy that event is flagged for further review.

A social security number is valid if it is a nine-digit number in the format “AAA-GG-SSSS”. The first 3 digit set of numbers are determined by an individual’s geographic location. The middle segment is the group number which can range from 01-99. The final segment is known as the serial number which can range from 0001-9999 and is assigned randomly to an individual.

The trigger requires the presence of a valid social security number, as determined by the assigning convention created by the SSA. Once a valid social security number has been identified, the trigger looks for information such as a zip code, a date of birth, a state of origin, or an address. After the policy finds one of these prerequisites, it looks for any additional social security numbers, or words such as "social security number", "SSN", or "his/her social". Once all of these conditions are met, the event is captured and flagged for review by a designated person to determine the severity of the violation.

Solicitations: Charitable

While an employer cannot dictate what an individual employee does outside of business hours, when in the workplace the focus should be on doing the job that the individual was hired for. Additionally, an employer may want to ensure that employees are not conducting personal/outside business on company time. In the United States, each state outlines specific regulations around solicitation and collection of funds for charitable purposes, where entities are required to go through specific processes and registrations before they are allowed to solicit donations for their cause. In order to hedge against potential fraudulent activity, and to ensure that the company is not held liable for an employee pursuing off duty activities during company time, the Solicitations: Charitable policy was created.

The Solicitations: Charitable policy is designed to capture activity associated with attempts to solicit general charitable contributions and donations.

The Solicitations: Charitable policy works by first identifying the mention of a charity name, donation cause, or method of raising funds. Once a match is found, the policy then searches for methods of contribution such as “make check payable to”, “Donate online”, or “click to make a contribution”. When a predetermined threshold is breached, the trigger fires and queues the event for review by an individual to determine the level of offense.

Solicitations: General

Another policy designed to prevent the misuse of company resources for the purposes of non-work related activities, the Solicitations: General policy captures employee communications involving an attempt to garner support, time, or funds for a non-company related cause, group, or activity.

The Solicitations: General policy works by identifying terms, words, phrases or expressions used when attempting to solicit something from someone else. Phrases such as “you should donate to …”, “would you like to contribute”, or “taking up a collection”, are searched for. Additionally, the policy looks for select phrases involving a few specific causes, or groups such as “Order Girl Scout Cookies”, “This is for my church/synagogue/temple”, or “Toys-for-Tots drop off”. Once a predetermined number of matches is identified, the trigger fires and the event is flagged for review.

Solicitations: Political

Campaign finance laws and regulations dictate contribution limits and identify the required disclosure forms for making contributions to political campaigns. To ensure that all contributions are within the guidelines as outlined by the US Federal government, and to ensure that the proper employees of a company are making the contribution on the company's behalf, we've created the Solicitations: Political policy.

The Solicitations: Political policy is designed to capture attempts to request money, or other forms of donations to political campaigns, from company employees. This policy, as opposed to the Dodd-Frank: Political contributions policy, focuses on attempts to garner donations, as opposed to an individual offering a donation.

The Solicitations: Political policy works by first identifying a mention of a political party (Democratic, Republican, Independent, etc.), or discussing the candidacy/campaign of an individual, by searching for wording such as "Political fundraiser", "Our candidate", "Running for Governor/Senator/President". Once such phrasing is identified, the policy looks for language around various types of donations such as "Volunteer your time", "Contribution amount", "Check payable to", or "Taking up a collection". When a predetermined threshold is reached, the trigger fires and flags the event for review by an individual to determine the level of offense.

Solicitations: Private Investments

FINRA Rule 3270 states "No registered person may be an employee, independent contractor, sole proprietor, officer, director or partner of another person, or be compensated, or have the reasonable expectation of compensation, from any other person as a result of any business activity outside the scope of the relationship with his or her member firm, unless he or she has provided prior written notice to the member, in such form as specified by the member. Passive investments and activities subject to the requirements of NASD Rule 3040 shall be exempted from this requirement." This rule outlines the requirement to disclose all outside business activities, of which private investments are included.

The Solicitations: Private Investments policy is designed to capture communications where employees are attempting to obtain services or monetary funds from another individual, be it an internal co-worker or external client, for the purposes of investing it in a non-company associated manner.

The Solicitations: Private Investments policy works by first identifying language associated with a financial transaction, instrument, or a method of funding such as "Wire the money to my account", "There's a partnership in it if you invest", "[quantity] shares/dollars/units". The policy then searches for language that includes types of investments and an indication that it's not company-related such as "Our Hedge Fund", "Private Investing", or "we can get a Personal Loan". Once a predetermined threshold is breached, the event is flagged for review.

Solicitations: Religious

While an employer cannot dictate what an individual employee does outside of business hours, when in the workplace the focus should be on doing the job that the individual was hired for. Additionally, an employer may want to ensure that employees are not conducting personal/outside business on company time. In the United States, each state outlines specific regulations around solicitation and collection of funds for charitable purposes, where entities are required to go through specific processes and registrations before they are allowed to solicit donations for their cause. In order to hedge against potential fraudulent activity, and to ensure that the company is not held liable for an employee pursuing the off duty activities during company time, the Solicitations: Religious policy was created.

The Solicitations: Religious policy captures activity of employees, or outside organizations, attempting to solicit a charitable donation for religious purpose from an individual at a company.

The Solicitations: Religious policy works by first identifying a religious group, or an organization's place of congregation, such as "the Church/Synagogue/Mosque/Parish" etc. Once a match is found, the policy then continues to search the communication for the indications of fund raising. This is accomplished by searching for language around "Needs your support", "Fundraiser", or "Asking for your help". Lastly the policy looks for a series of positive language indicators that the individual should donate money such as "Tithing", "Pledge [Amount of money] today", or "Contribute to the Church/Synagogue/Mosque/Parish". Once a predetermined threshold of events is reached, the policy flags the event for review by an individual to determine the level of offense.

Taiwan Identity Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Taiwan Identity Card Number policy captures the unauthorized distribution and dissemination of Taiwan's version of the United States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Taiwan Identity Card Number policy works by first identifying the mention, or otherwise labeling, of the information in the communication ("National ID","國民身分證", " Guómín Shēnfènzhèng"), in both its English translation, the native character set, and the roman character set for Mandarin, the nation language of Taiwan. Once this condition is met, the policy uses a pattern matching definition to identify Taiwan Identity Card Numbers in various formats. When both of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Tax Advice Prohibition

Circular 230, found in Title 31 of the Code of Federal Regulations Subtitle A Chapter Part 10 Subpart B §10.37, is a publication of regulations which include the rule governing requirements for written advice. The rule states that "A practitioner may give written advice (including by means of electronic communication) concerning one or more Federal tax matters" However "The practitioner must— (i) Base the written advice on reasonable factual and legal assumptions (including assumptions as to future events); (ii) Reasonably consider all relevant facts and circumstances that the practitioner knows or reasonably should know; (iii) Use reasonable efforts to identify and ascertain the facts relevant to written advice on each Federal tax matter; (iv) Not rely upon representations, statements, findings, or agreements (including projections, financial forecasts, or appraisals) of the taxpayer or any other person if reliance on them would be unreasonable; (v) Relate applicable law and authorities to facts; and (vi) Not, in evaluating a Federal tax matter, take into account the possibility that a tax return will not be audited or that a matter will not be raised on audit."

The Tax Advice Prohibition policy ensures that not only is the client receiving the best possible advice to promote a positive working relationship, but that only individuals who are legally authorized are offering said advice.

The Tax Advice Prohibition policy works in two layers. First, a communication is scanned for language indicative of a suggestion or recommendation, such as "I would urge you to", "I would suggest/recommend", "it's my opinion", or "you should/shouldn't do…" Once a match is identified, the policy then searches for the presence of various forms, methods, or sources of income, including but not limited to annuities, bonds, commodities, derivatives, property, mutual funds, and various other public or non-public investments. Once a predetermined threshold of matches is reached, the trigger fires and queues the event for review, where an individual will determine the severity of the violation.

Technical Specifications or Designs

In § 120.10 of the International Traffic in Arms Regulations (ITAR) the term “technical data” is defined as “Information, other than software as defined in **§** 120.10(a)(4) which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.” It is also defined as “Classified information relating to defense articles and defense services, information covered by an invention secrecy order.” In Part 125 § 125.3 it states “A request for authority to export defense articles, including technical data, classified by a foreign government or pursuant to Executive order 12356, successor orders, or other legal authority must be submitted to the Directorate of Defense Trade Controls for approval.” The Canadian Defense Production covers Technical Data Control Regulations and defines technical data as “'array of design or manufacturing know-how' means the know-how and related technical information required to achieve a development, production, or utilization purpose and includes any service, processed, procedures, specifications, design data, and criteria and testing techniques required to achieve such development, production, or utilization purposes.” This regulation outlines the requirement that any exported data that is not scientific, educational, or not a part of the public domain needs to be certified by the Canadian government before release in accordance with the United States Department of Defense directive, number 5230.25 regarding the withholding of unclassified technical data from public disclosure. In addition, the general security of proprietary information is of paramount importance to any firm. Email surveillance provides a comprehensive preventative solution to ensure such data loss.

The intent of the Technical Specifications and Designs policy is to analyze email, either sent or received, for any proprietary information relating to technical data as defined by the numerous security regulations surrounding. These regulations generally require a certification, a license, or the explicit approval of a government body or government official before any technical data is distributed to another firm, another country, or the general public domain. In many cases intellectual property can be more valuable than a company's end product. The policy uses multiple key words and contextual phrases to determine if an email or attachment contains references to intellectual property, thereby ensuring the security of such data that is not covered by the definitions outlined in the regulations.

The Technical Specifications and Designs trigger works by analyzing a communication for specific words or phrases that indicate the correspondence contains technical data. Such phrases include “Here are the technical drawings”, “Top/Bottom/side view”, “It requires 1.21 Gigawatts to power”, or any mention of size or specific dimensions. Once the customer defined threshold of matches is reached, the trigger fires and flags the event for review by a person who will determine the severity of the offense. We also recommend that before you release the policy into a production environment, you work with a policy technician to modify the policy to more specifically suit the your needs (i.e. creating a pattern matching definition to specifically target a document) and to increase the accuracy of the policy.

Termination/Layoff Discussions

Employee layoffs and terminations are an unfortunate, yet sometimes necessary, part of business. The Worker Adjustment and Retraining Notification (WARN) act states that Employers must give a minimum of 60 days' notice to Employees before executing a "Mass Layoff" (500 employees or greater or 33% or greater for companies with less than 500 employees). This regulation is for the benefit of the employees, to allow them sufficient time to prepare for the layoff. Information such as layoff dates is extremely time sensitive and should only be released when an authorize individual allows it. Discussion around terminations, between employees, are both distracting and damaging to company moral in general. The surveillance of electronic communications provides a viable solution to hedge against any risk associated with such discussions.

The Termination/Layoff Discussions policy is classified as an employee behavior monitor. The policy is intended to monitor and alert a reviewer if a user's communication activity contains information regarding terminations, indications that a layoff may occur, or rumors and speculations relating to the subject of employee termination or layoffs

The Termination/Layoff Discussions trigger works by monitoring for language that is indicative, or speculative in nature, along with language mentioning termination. Some phrases that would be captured include "We might have to cut back on staff", "Performance evaluations weren't good, I hear", or "I think they might be eliminating John's position". Language indicating that the termination is happening over electronic communication such as "Clean out your desk and go home", "Your benefits will continue for the rest of the month", or "We will no longer be needing your services" is also captured. When a customer-determined threshold of matches has occurred, the event is flagged for review.

Thailand Population Identification Code

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Thailand Population Identification Code policy captures the unauthorized distribution and dissemination of Thailand's version of the United States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Thailand Population Identification Code policy works by utilizing policy's pattern matching capabilities to identify Thailand's Population Identification Code in its proper format. Unlike many kinds of information that can follow the same pattern, such as a 10 digit US phone number or 10 digit account number, the Thailand Population Identification Code number has a unique format. Therefore, this allows us to search for the number by itself, without the communication containing a mention of a Thailand PIC. Once a match is identified, the policy flags the event for review by an individual to determine the severity of offense.

Threats of Litigations

The Fair Debt Collection Practices Act [15 USC 1692e] § 807 states that “A debt collector may not use any false, deceptive, or misleading representation or means in connection with the collection of any debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:” “(5) The threat to take any action that cannot legally be taken or that is not intended to be taken”. Inversely, any lawsuit filed against a company by a customer, no matter how big or small, is a serious issue that can result in a variety of consequences such as large pay-outs, customer loss, or reputational damage. It is imperative that such a situation is escalated to the proper individuals and handled delicately to maintain control of the situation.

The Threats of Litigation policy is intended to monitor incoming and outgoing communications to prevent employees from making threats to customers illegally as part of the FDCPA regulation, in addition to monitoring incoming threats from customers relating to consumer dissatisfaction. The policy looks for specific discussions that indicate an outside party or internal personnel suggesting, or outright threatening, legal action.

The Threats and Litigation trigger looks for a type of coercive or aggressive threatening language such as “You’ll be hearing from my attorney”, “We intend to sue”, “We’re going to put you out of business”, or “I’ll sue you for everything you’re worth”. When a customer-determined threshold of matches is reached, the trigger fires and flags the event for review to determine the severity of the infraction.

UK Driver's License

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The UK Driver's License policy is designed to look for individuals unlawfully distributing sensitive client information, which is typically contained in a driver's license.

The UK Driver's License policy works policy works by first scanning a communication either for the mention of a driver's license or country or a type of license, such as a CDL. Once this condition is met, the policy uses a pattern matching definition to identify and validate UK driver's license numbers in various formats. When all of these conditions are met, the policy triggers and flags the event for review by an individual.

UK Driver's License - Threshold

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The UK Driver's License - Threshold policy is designed to look for individuals unlawfully distributing sensitive client information, which is typically contained in a driver's license. This threshold version is specifically used to capture multiple instances, as in the case of individuals disseminating client lists, database exports, or spreadsheets containing sensitive information.

The UK Driver's License – Threshold policy works by first scanning a communication either for the mention of a driver's license or country, or a type of license, such as a CDL. Once this condition is met, the policy uses a pattern matching definition to identify and validate UK driver's license numbers in various formats. When a specific quantity of matches is identified, and the threshold reached, the policy triggers and flags the event for review by an individual.

UK Employee Compensation Information

The UK Employee Compensation Information policy is a class of employee behavior policies meant to enforce proper etiquette, in terms of discussing salary.

The UK Employee Compensation Information policy works by identifying language around mentioning tax reporting forms, alternate forms of income, paycheck deductions, or tax codes indicative of level of income. Once a predetermined threshold is reached, the trigger fires and flags the event for review by an individual to determine the level of offense.

UK National Insurance Number

According to the Freedom of Information Act (section 40 and regulation 13) and the Data Protection Act, “personal data” is defined as “data which relates to a living individual who can be identified” Under English regulation, the National Insurance Number is considered to be personal data. The regulation continues to state “Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.”

The UK National Insurance Number identifies the holder as a UK resident registered and entitled to the benefits afforded by the UK National Health System. It is occasionally also used for identification purposes, since each number is unique. The National Insurance Number is an alpha-numeric string consisting of two leading letters, six digits and a trailing letter. This policy scans for the appropriate string construction, including the proper leading alphabetic characters and sequences to ensure that the string in question is in fact a UK National Insurance Number. With that determination, scanning continues for other contextual elements and phrases (such as HM Revenue & Customs, NINO, etc.) to confirm the instance and reduce false positives.

The UK National Insurance Number trigger works by analyzing a communication for the presence of terms that may indicate an email contains a national insurance number such as “ID number”, “Insurance #”, “NINO”, or “Deductions Working Sheet”. Once at least one of these terms is matched, the trigger then continues to scan for the presence of a national insurance number in numerous formats. When these two conditions are met, the trigger fires and flag the event review.

UK National Insurance Number – Threshold

The definition of personal data, as defined in the UK Data Protection Act of 1998, is “data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.” The act also defines the conditions in which the data is allowed to be used. In the UK the National Insurance Number is a "personal account number” used in the administration of the National Insurance or social security system, and is also used for some purposes in the UK tax system. Because it is a unique number allocated to almost every adult resident of the country it can also be used for the purposes of identity verification.

The UK National Insurance Number – Threshold policy uses a custom pattern matching definition to identify the standard format of the UK national insurance number. This threshold version is specifically used to capture multiple instances, as in the case of individuals disseminating client lists, database exports, or spreadsheets containing sensitive information.

The UK National Insurance Number – Threshold policy works by looking for phrasing that identifies the information as a national insurance number or suggests its use , such as “ID Num”, “Nat ins”, or “Tax return”. Once this condition is met, the policy uses a pattern matching definition to identify a UK National Insurance Number in various formats. This pattern can appear in one of several formats, as many are commonly used to express insurance numbers. Once a predetermined threshold is breached, the policy triggers and identifies the event for review by an individual to determine the validity of the violation.

UK National Insurance Number with Additional PII

The definition of personal data, as defined in the UK Data Protection Act of 1998, is “data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.” The act also defines the conditions in which the data is allowed to be used. In the UK the National Insurance Number is a "personal account number” used in the administration of the National Insurance or social security system, and is also used for some purposes in the UK tax system. Because it is a unique number allocated to almost every adult resident of the country it can also be used for the purposes of identity verification.

The UK National Insurance Number with Additional PII policy uses a custom pattern matching definition to identify the standard format of the UK national insurance number in addition to information with which one can identify an individual.

The UK National Insurance Number with Additional PII works by verifying that a communication contains a match to the national insurance number pattern. Once a match has been identified, the policy then searches for additional PII (for example the mention of information such as date of birth, generic column headers, postal codes, or other indications of a generic address). Next, the policy searches for a mention of “ID number”, various forms that could contain the aforementioned information, or other use cases for the information (i.e. tax returns). Once all three of these conditions are met, the policy triggers and flags the event for review by an individual to determine the severity of the violation.

UK Resumes/CVs

It is generally understood that employees should not apply for positions at other companies through their current employer's channels of communication. Doing this is not only bad for the employee, as it says to the company they are applying to "I'm applying for jobs on my current company's time, using my current company's resources (and will do the same to you) and I don't see that there's anything wrong with this" but it is also projects a poor image of the employee's current employer.

The UK Resumes/CVs policy scans for forms of PII used in resumes and curriculum vitae, such as address and phone number, education and references to employment/employment history, skills, interests, etc. Capturing employee attempts to send out resumes from their company addresses can avoid potential reputational and morale damage to the firm.

The UK Resumes/CVs trigger looks for at least one instance of CV, Curriculum Vitae, date of birth, experience, or marital status. It is important to note that only one of these pieces of information is required, though any combination may be present. The Second piece of information is a reference to some level of education such as a degree type, "BA", "PhD", "MBA", "NQF" etc., or the mention of a university or college. The final piece of required information is a reference to former employment such as the mention of "Employment History", "Professional Experience", or "Work history" within 25 words of a date range in various formats such as "10/1 – 14/4" or "Jan 07 thru Oct 10" etc. Once the trigger matches on all three pieces of information the trigger fires and the event is placed in a queue for review.

UK Tax Identification Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The UK Tax Identification Number policy is a DLP (data loss prevention) policy intended to capture the unauthorized dissemination of tax information, as it is used in the UK.

The UK Tax Identification Number policy is designed to first identify the mention of "VAT identification" or "Value Added Tax". Once it's confirmed in the communication, the policy then uses a pattern matching definition to validate a VAT ID number. When a predetermined quantity of VAT numbers is identified, the policy flags the event for review by an individual.

UK Tax Identification Number - Threshold

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The UK Tax Identification Number – Threshold policy is a DLP policy intended to capture the unauthorized dissemination of tax information, as it is used in the UK. This threshold version is specifically intended to capture multiple instances, as in the case of individuals disseminating client lists, database exports, or spreadsheets containing sensitive information.

The UK Tax Identification Number – Threshold policy is designed to first identify the mention of "VAT identification" or "Value Added Tax". Once it's confirmed in the communication, the policy then uses a pattern matching definition to validate a VAT ID number. When a predetermined quantity of VAT numbers is identified, the policy flags the event for review by an individual.

Unencrypted Wire Transfer Information

Federal Regulation J, Article 4A of the Uniform Commercial Code (UCC), The Payment Card Industry Security Standards Council Regulations (PCI) and FDIC Regulation 6500 Title IX (Electronic Fund Transfer Act) outline the various requirements regarding the procedures involved in wire transfers. Federal Regulation J and the Electronic Fund outline the procedures by which transfers need to occur to ensure the security of the customer's information. The PCI standard states the requirement for encryption of any electronically transmitted payment card information whether at a terminal such as an ATM, or sending the physical information through electronic communication. Article 4A of the UCC defines "security procedure" as "a procedure established by agreement of a customer and a receiving bank for the purpose of verifying that a payment order or communication amending or cancelling a payment order is that of the customer" and "may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices."

Using keywords and phrases such as wire, transfer, sending, account, currency, beneficiary, moved, etc. in the proper order, and in combination with bank routing numbers, the Unencrypted Wire Transfer Information Policy identifies the disclosure of an unencrypted wire transfer. The intent of this policy is to ensure that such information is handled properly, not only for regulatory compliance, but to ensure the satisfaction and trust of the client's customers. The client has the option to allow this information to flow, to force encryption before sending, or to prevent the email from being sent.

The Unencrypted Wire Transfer Information trigger scans a document in 3 stages. The policy requires that words such as "Wire transfer", "Wired $5,000" (or any amount of money), or "Bank transfer" be present in the communication. Once this requirement is fulfilled, the trigger scans the correspondence for additional pre-qualifying words and phrases such as "ABA number", "BIC code", or "Routing information". When the trigger matches at least one pre-qualifier, it then searches for a combination of terms relating to wire instructions such as "To be deposited for", "Receiving Account", or number patterns that may indicate routing codes or account numbers. Once a customer-determined threshold of matches is found, the trigger flags the email for review.

Unqualified Rebates or Benefits

Another policy that monitors for fair business practices and customer relations, the Unqualified Rebates or Benefits policy, screens for the activity of employees offering bribes in the form of benefits or rebates, which are unauthorized or otherwise unredeemable.

The Unqualified Rebates or Benefits policy searches for language which would indicate such an offering. Terms and phrases like “Honor the terms”, “If you buy exclusively from us”, “They’re receiving payment from us”, or “withholding the rebate until you buy from us” are all identifiers of a violation. Once a predetermined threshold of comments like these is met, the policy flags the event for review by an individual to determine the severity of offense.

US Driver's License

According to 5 U.S. Code § 552a, regarding records maintained on individuals, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties"

Information such as US driver's license information is subject to this regulation due to the sensitive and personally identifiable information contained in a driver's license. The US Driver's License policy is intended to prevent or monitor the distribution/transmission of private information whether sent accidentally or maliciously. The US Driver's License trigger inspects for number strings and language that indicate this particular form of PII. For US Drivers Licenses, the trigger scans for state abbreviations and the associated formatted numbers strings that identify a driver's license number.

The US Driver's License trigger works by first analyzing a communication for the presence of information that could indicate a driver's license such as the literal mention of "Driver's License" or a license classification such as "CDL". Once one of these has been identified, the trigger then continues to scan for specific patterns such as the mention of a state within five objects of a 7 to 12 digit number or a number symbol (#) within in 5 objects of a 2 to 5 digit number adjacent to a state code. Once a customer determined threshold of matches is identified, the trigger fires, captures the event, and flags it for review by an individual.

US Driver's License - Threshold

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The US Driver's License – Threshold policy captures communications that may contain personally identifiable information that is typically found on a driver's license. This threshold version is specifically used to capture multiple instances, as in the case of individuals disseminating client lists, database exports, or spreadsheets containing sensitive information.

The US Driver's License – Threshold policy works by first scanning a communication either for the mention of a driver's license or state, or a type of license, such as a CDL. Upon finding a match, the policy then looks for numbers that correspond to a US Driver's license number in a variety of formats and tallies the occurrences. When a threshold of matches is reached, the trigger fires and flags the event for review to determine the severity of the issue.

US Employee Compensation Information

Uncontrolled dissemination of employee compensation can be detrimental to any organization. Most companies have established internal policies stating that employees are prohibited from discussing their salary or wage levels and company benefits with employees inside or outside of the firm. While it is technically not illegal for employees to discuss compensation information, it can be demoralizing and detrimental to the professional environment.

The US Employee Compensation Information policy is intended to monitor discussions among surveilled users, or discussions with external groups or individuals, that involve various forms of payment such as pay rate, total compensation, stock options, hourly/annual rate, salary, job offers etc. This is primarily to prevent potentially hostile work environment situations domestically and to ensure such sensitive financial information, which could damage the professional atmosphere or reputation of the company, remains secure.

The US Employee Compensation Information trigger works by analyzing an email for the presence of language discussing various forms of compensation and the receiving of said compensation such as “I make 25 an hour here”, “They gave me some good stock options”, “My gross salary for the year ends up being 120,000 dollars”, or “John Smith is getting a sizable benefits package”. Once a customer-determined threshold of matches is identified, the trigger fires and flags the event for review.

US Individual Taxpayer Identification Number (ITIN)

Any customer that divulges personal information for the purposes of doing business does so with the understanding that their information will be kept confidential. This makes the security of sensitive customer information an imperative in an enterprise environment. Failing to do this can result in reputational damage, loss of customers, regulatory fines, or the revocation of a license to do business.

The US Individual Taxpayer Identification Number (ITIN) is a processing number issued by the Internal Revenue Service (IRS) for the purpose of federal tax reporting. It is a nine-digit number that always begins with the number 9 and has a range of 70-80 in the fourth and fifth digit. As of April 12, 2011, the range was extended to include 900-70-0000 through 999-88-9999, 900-90-0000 through 999-92-9999, and 900-94-0000 through 999-99-9999.

The US Individual Taxpayer Identification Number (ITIN) policy analyzes a communication for the presence of a valid ITIN number as outlined in the assigning convention created by the IRS. If a valid number is identified the trigger then looks for corroborating information establishing the number as an ITIN such as "TIN", "ITIN", "This is her tax ID", or "FEIN" in the same location (i.e. both being in the body of an email or both present in the same document that is attached to an email). If a valid ITIN is identified and there is no information in the email stating in some way that it is an ITIN, or if a valid ITIN is discovered and the identifying information ("ITIN", "FEIN", or "Tax ID" etc.) is not contained in an attachment, the trigger will not fire.

When the policy captures an event it is flagged for review by a designated person to determine if the event is a violation.

US Individual Taxpayer Identification Number (ITIN) – Threshold

Any customer that divulges personal information for the purposes of doing business does so with the understanding that their information will be kept confidential. This makes the security of sensitive customer information an imperative in an enterprise environment. Failing to do this can result in reputational damage, loss of customers, regulatory fines, or the revocation of a license to do business.

The US Individual Taxpayer Identification Number (ITIN) is a processing number issued by the Internal Revenue Service (IRS) for the purpose of federal tax reporting. It is a nine-digit number that always begins with the number 9 and has a range of 70-80 in the fourth and fifth digit. As of April 12, 2011, the range was extended to include 900-70-0000 through 999-88-9999, 900-90-0000 through 999-92-9999, and 900-94-0000 through 999-99-9999.

The US Individual Taxpayer Identification Number (ITIN) – Threshold policy analyzes a communication for the presence of several (or a threshold amount) of valid ITIN numbers as outlined in the assigning convention created by the IRS. If a valid number is identified the trigger then looks for corroborating information establishing the number as an ITIN such as "TIN", "ITIN", "This is her tax ID", or "FEIN" in the same location (i.e. both being in the body of an email or both present in the same document that is attached to an email). If a valid ITIN is identified and there is no information in the email stating in some way that it is an ITIN, or if a valid ITIN is discovered and the identifying information ("ITIN", "FEIN", or "Tax ID" etc.) is not contained in an attachment, the trigger will not fire. This version of the ITIN policy looks for a specific amount of taxpayer identification numbers which could be indicative of an individual attempting to distribute a list which could also contain other sensitive information.

When the policy captures an event it is flagged for review by a designated person to determine if the event is a violation.

US Passport Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The US Passport Number policy is a broadly defined policy intended to capture the unlawful distribution of passport numbers in various formats.

The US Passport Number policy looks for two items in a communication. The mention of a "passport", "passport number", and variations thereof, and a nine digit number either formatted or unformatted. Once these two elements are identified, the policy triggers and flags the event for review by an individual to determine the severity of the violation.

US Passport Number - Threshold

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The US Passport Number - Threshold policy is a broadly defined policy intended to capture the unlawful distribution of passport numbers in various formats. This threshold version is specifically used to capture multiple instances, as in the case of individuals disseminating client lists, database exports, or spreadsheets containing sensitive information.

The US Passport Number policy looks for two items in a communication. The mention of a "passport", "passport number", and variations thereof, and a nine digit number either formatted or unformatted. Once several instances of these two elements are identified in a communication, the policy triggers and flags the event for review by an individual to determine the severity of the violation.

US Resumes/CVs

It is generally understood that employees should not apply for positions at other companies though their current company's channels of communication. Doing this is not only bad for the employee, as it says to the company they are applying to "I'm applying for jobs on my current company's time, using my current companies resources (and will do the same to you) and I don't see that there's anything wrong with this" but it is also projects a poor image of the employee's current employer.

The US Resumes/CVs policy scans for forms of PII used in resumes and curriculum vitae, such as address and phone number, education and references to employment/employment history, skills, interests, etc. Capturing employee attempts to send out resumes from their company addresses can avoid potential reputational and morale damage to the firm.

The US Resumes/CVs trigger specifically looks for 3 pieces of information that are present on every resume. The first piece of information is either a US formatted zip code, either 12345 or 12345 - 1234, or a formatted phone number with an area code. It is important to note that only one of these pieces of information is required, both can be present but only one is needed. The Second piece of information is a reference to some level of education such as a degree type, "BA", "PhD", "MBA" etc., or the mention of a university or college. The final piece of required information is a reference to former employment such as the mention of "Employment History", "Professional Experience", or "Work history" within 25 words of a date range in various formats such as "1/10 - 4/14" or "Jan 07 thru Oct 10" etc. Once the policy matches on all three pieces of information the trigger fires and flags the event for review.

Vietnam ID Card Number

Countless regulations and laws exist in the United States, Europe, and across the world that protect information that can be used to verify an individual's identity. Laws such as The Privacy Act of 1974, The Health Insurance Portability and Accountability Act, The Payment Card Industry Data Security Standards, The Fair Credit Reporting Act, The Data Protection Act of 1984, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Personal Information Protection and Electronic Documents Act, are intended to establish the security standards by which corporations, and other entities which operate in the US, Canada, or Europe, handle, distribute, and protect personally identifiable information.

The Vietnam ID Card Number policy captures the unauthorized distribution and dissemination of Vietnam's version of the Unite States' Social Security number. This ensures against data breaches, which can effectively damage the reputation of a company, and compromise sensitive client information.

The Vietnam ID Card Number policy works by first identifying the mention, or otherwise labeling, of the information in the communication ("Vietnam ID"," Giấy chứng minh nhân dân", "vietnam carte d'identité"), in its English translation, its French Translation, and in Vietnamese, the language of Vietnam. Once this condition is met, the policy uses a pattern matching definition to identify Vietnam ID Card Numbers in various formats. When both of these conditions are met, the policy flags the event for review by an individual to determine the severity of the offense.

Wallcrossers

The National Association of Securities Dealers and the New York State Stock Exchange (NASD/NYSE) memo 91-45 outlines the "'minimum elements' of adequate Chinese Wall policies and procedures pursuant to the requirements of the Insider Trading and Securities Fraud Enforcement Act of 1988". The memo goes on to state that "These minimum elements include review of employee and proprietary trading, memorialization and documentation of firm procedures, substantive supervision of inter-departmental communication by the firm's compliance department, and procedures concerning proprietary trading when the firm is in possession of material, non-public information." Part III of the memo reference NYSE Rule 342 and 351 which state the requirements that members (Financial Entities) must meet to perform their due diligence regarding both communication and trading surveillance.

The Wallcrossers policy is intended to hedge the risk associated with bringing public facing employees over the Chinese wall to collaborate and exchange information with the associated private-facing Deal Team Members. The policy focuses on communications from individuals that are registered and approved wall crossers being sent to either a private-side employee, who is not a member of a deal team, or any other public side employee. This includes other wall crossers that are not part of the same deal team.

The Wallcrossers policy applies only to communications sent from a wall crosser to any public side or non- deal team recipient (i.e. the policy would apply whether Tom (wallcrosser) sends an email to just Jane (public), or to Joe (deal team), Frank (deal Team), and Jane (public)). Once this condition is met, the policy looks for a comprehensive range of language such as "I hear that company will…", "Rumor has it that…", "Between you and I…", "You're sworn to secrecy", "You scratch my back…", "I do… for you, you do… for me", "Not over the wall but can I send…", "Haven't been approved but can I attend the meeting", "Should they be over the wall for this". Due to the narrow specificity of the communication participants, the policy only requires one match before the trigger fires and the event is captured for review.

Whistleblower

The Exchange Act 15 U.S.C. 78u-6 defines a whistleblower as “an individual who provides, or 2 or more individuals acting jointly who provide, information relating to a violation of the securities laws to the Commission, in a manner established, by rule or regulation, by the Commission.” Section 6(h)(1) states that “No employer may discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment because of any lawful act done by the whistleblower.” The Securities and Exchange Commission Regulation 21F 240.21 outlines the guidelines by which whistleblowers can submit information to the SEC regarding violations and be classified as a whistleblower thereby entitling them to all the rights, privileges, and rewards thereof. Regulation 21F 240.21F-9 states that “to be considered a whistleblower under Section 21F of the exchange act, you must submit your information about a possible securities law violation by either of these methods: (1) Online, through the Commission’s website located at www.sec.gov; or (2) By mailing or faxing a Form TCR (Tip, Complaint, or Referral) to the SEC Office of the Whistleblower”.

The Whistleblower policy is intended, not to prevent employees from whistleblowing on their employer, but to ensure that the employee attempting to distribute such information is allowed to do so through the proper channels to ensure that they are eligible for all legal rights granted to whistleblowers. The policy looks for a possible whistleblower situation and allows an organization to take appropriate steps in response to this information.

The Whistleblower trigger works by scanning electronic communications for language that may indicate the individual's intention to whistle blow, such as “They are lying to the regulators”, “Violating NASD Rule 2030”, or “The information that I bring is unethical and is in direct violation of NASD regulations”. When a customer-determined threshold of matches is reached, the trigger fires and flags the event for further review to determine the level of severity.