Committing to Ethics and Managing Risk

2017

Interactive PDF

Your Commitment
Code of Conduct
Seeking Advice
Policies
Pre-Clearance
Government Resources

Ethics - Your Commitment

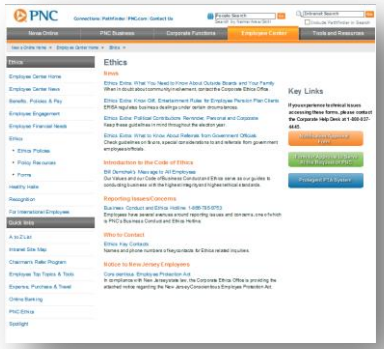
PNC's culture is built on a foundation of seven Values – Performance, Customer Focus, Respect, Teamwork, Integrity, Diversity, and Quality of Life – and strength of our commitment to always do what is right by those we serve. PNC's Code of Business Conduct and Ethics (Code) serves as the basis for doing what is right, doing what is ethical.

The Code and related ethics policies provide guidance to employees in conducting daily business activities. This guide serves as a reminder of our commitment to ethical and appropriate behavior. Anything less is unacceptable.

- ✔ Always act in a professional, respectful, and honest manner when conducting activities with and on behalf of PNC.
- ✔ Understand and follow our Code, related ethics, human resources, and compliance policies, and any other policies that pertain to our job responsibilities.
- ✔ Ask questions of, or raise concerns with, the appropriate individuals.
- ✔ Provide all required notifications and obtain necessary approvals.

Ethics – Website

Click on the thumbnail to access the Ethics site on the PNC Intranet.



Ethics – Seeking Advice

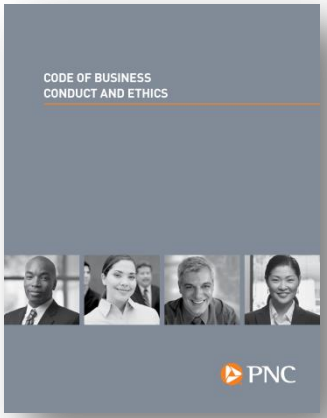
There are people who are available to help when you have questions or concerns about the Code or other business conduct issues:

- ✔ Your manager
- ✔ The Corporate Ethics Office at **412-768- 8507**
- ✔ The PNC Business Conduct and Ethics Hotline **at 1-866-785-9753, where you may remain anonymous**
- ✔ The Corporate Ethics Office mailbox at: **Corporate.Ethics.Office@pnc.com**
- ✔ The Employee Relations Information Center (ERIC) at **1-877-968-7762**
- ✔ The ERIC mailbox at **ERIC@pnc.com**

Your Commitment
Code of Conduct
Seeking Advice
Policies
Pre-Clearance
Government Resources

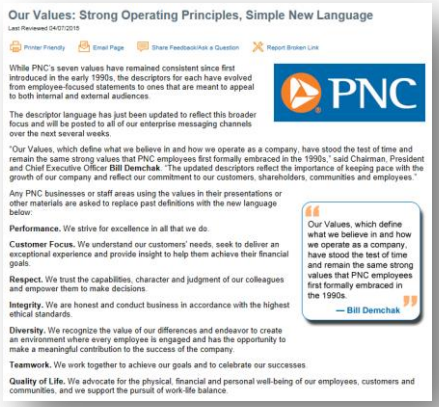
Ethics – Code of Conduct

Click on the thumbnail to access the Code.



Ethics – Values

Click on the thumbnail to access a list of our Values.


Our Values: Strong Operating Principles, Simple New Language

Last Reviewed 04/07/2015

Printer Friendly | Email Page | Share Feedback/Ask a Question | Report Broken Link

While PNC's seven values have remained consistent since first introduced in the early 1990s, the descriptors for each have evolved from employee-focused statements to ones that are meant to appeal to both internal and external audiences.

The descriptor language has just been updated to reflect this broader focus and will be posted to all of our enterprise messaging channels over the next several weeks.

"Our Values, which define what we believe in and how we operate as a company, have stood the test of time and remain the same strong values that PNC employees first formally embraced in the 1990s," said Chairman, President and Chief Executive Officer **Bill Demchak**. "The updated descriptors reflect the importance of keeping pace with the growth of our company and reflect our commitment to our customers, shareholders, communities and employees."

Any PNC businesses or staff areas using the values in their presentations or other materials are asked to replace past definitions with the new language below:

Performance. We strive for excellence in all that we do.

Customer Focus. We understand our customers' needs, seek to deliver an exceptional experience and provide insight to help them achieve their financial goals.

Respect. We trust the capabilities, character and judgment of our colleagues and empower them to make decisions.

Integrity. We are honest and conduct business in accordance with the highest ethical standards.

Diversity. We recognize the value of our differences and endeavor to create an environment where every employee is engaged and has the opportunity to make a meaningful contribution to the success of the company.

Teamwork. We work together to achieve our goals and to celebrate our successes.

Quality of Life. We advocate for the physical, financial and personal well-being of our employees, customers and communities, and we support the pursuit of work-life balance.

PNC

"Our Values, which define what we believe in and how we operate as a company, have stood the test of time and remain the same strong values that PNC employees first formally embraced in the 1990s."
— Bill Demchak

PNC's Code of Business Conduct and Ethics ("Code") documents our ethics standards and demonstrates our commitment to ethics and values. It defines expectations and provides guidelines for conducting business on behalf of PNC.

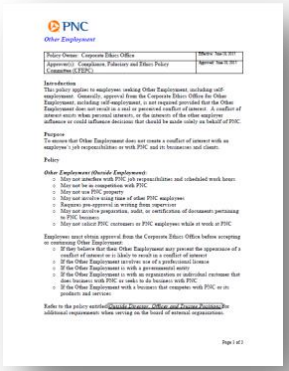
The Code is a resource for all PNC employees. It helps to identify situations where our Values might be at risk or where there may be a potential violation of the Code.

Your Commitment
Code of Conduct
Seeking Advice
Policies
Pre-Clearance
Government Resources

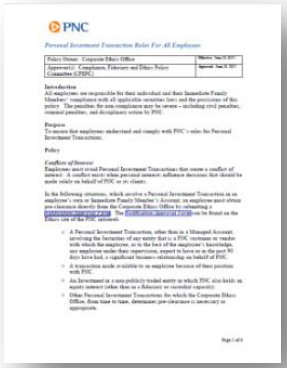
Ethics Policies

Click on a thumbnail to access the associated policy and procedures.

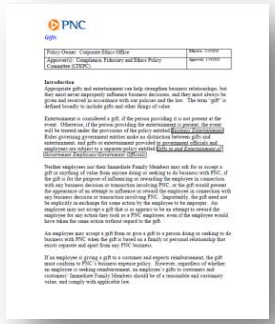
Other Employment



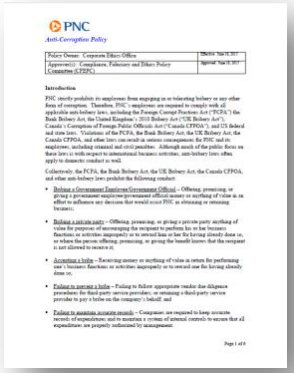
Personal Investment Transaction Rules



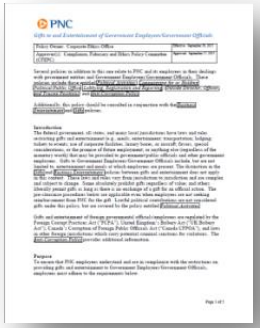
Gifts



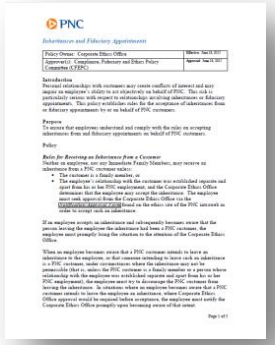
Anti-Corruption Policy



Gifts to and Entertainment of Government Employees



Inheritances and Fiduciary Appointments

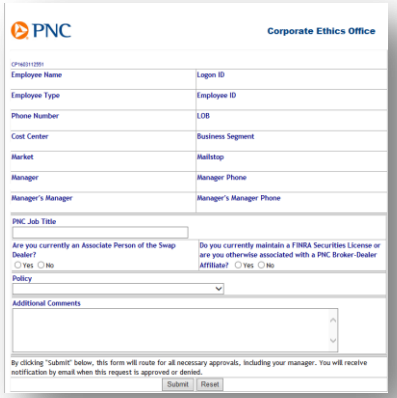


Your Commitment
Code of Conduct
Seeking Advice
Policies
Pre-Clearance
Government Resources

Ethics – Pre-Clearance

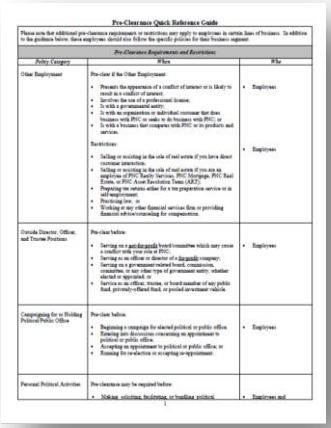
Click on the thumbnails below for assistance with pre-clearance.

Pre-Clearance Notification/Approval Form


PNC Corporate Ethics Office

Employee Name | Logon ID
Employee Type | Employee ID
Phone Number | LOB
Cost Center | Business Segment
Market | Mailstop
Manager | Manager Phone
Manager's Manager | Manager's Manager Phone
PNC Job Title
Are you currently an Associate Person of the Swap Dealer? ○ Yes ○ No
Do you currently maintain a FINRA Securities License or are you otherwise associated with a PNC Broker-Dealer Affiliate? ○ Yes ○ No
Policy
Additional Comments
By clicking "Submit" below, this form will route for all necessary approvals, including your manager. You will receive notification by email when this request is approved or denied.
Submit | Reset

Pre-Clearance Quick Reference Guide


Pre-Clearance Quick Reference Guide

Ethics – Government Policy Resources

Lobbying Requirements

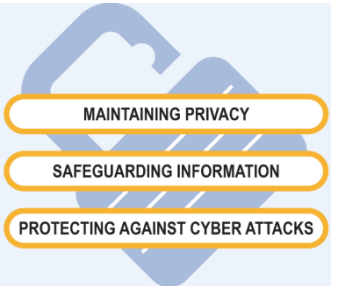
Lobbyist Thresholds

Pre-Clearance Political Contributions Chart

Your Commitment
Privacy Policy
Security Home Page
Security Policy / Tips
Get Help and Report
Additional Resources

Privacy and Security – Your Commitment

As a member of the PNC team, there is an expectation that you are committed to protecting confidential and personal information from improper disclosure, theft, loss and abuse.



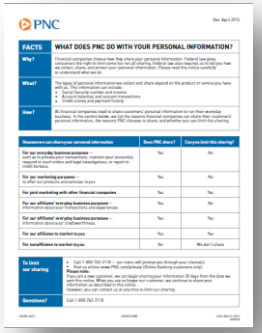
You can do this by:

- ✔ Maintaining the privacy of every PNC customer and employee
- ✔ Safeguarding all confidential information – all the time, everyday
- ✔ Protecting against cyber attacks that are aimed at accessing PNC confidential information

Privacy Notice and Policy

Privacy Notice

This document, which must be provided to consumers, states our corporate position regarding the use and management of their personal information.


PNC

FACTS WHAT DOES PNC DO WITH YOUR PERSONAL INFORMATION?

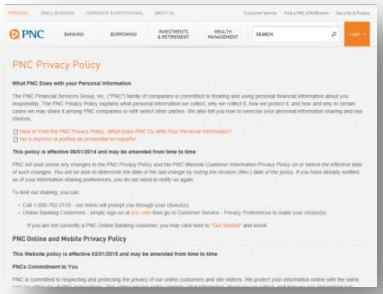
Why?

What?

How?

Online Privacy Policy

This document denotes how personal data may be used in an online or mobile setting.


PNC

PNC Privacy Policy

What PNC Does with your Personal Information

PNC Online and Mobile Privacy Policy

PNCs Commitment to You

Cyber Security – Home Page

Your Commitment
Privacy Policy
Security Home Page
Security Policy / Tips
Get Help and Report
Additional Resources

News Articles

Cyber Security Policies and Procedures

Quick and Fun Cyber Security Learning Games

Ask Cyber Security Blog Posts

Phishing Educational Page

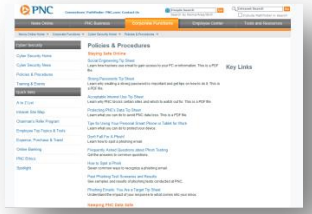
Cyber Security Services

February 8, 2017 (P&S Version)

Your Commitment
Privacy Policy
Security Home Page
Security Policy / Tips
Get Help and Report
Additional Resources

Security – Policy and Tips

Cyber Security Policies and Procedures



Strong Passwords Tip Sheet

Protecting PNC's Data Tip Sheet

Tips for Work Area, PC, and Laptop Security

Mobile Security Tip Sheet

New Transmission Form

Social Media Tip Sheet

Foreign Travel Guidelines and Tip Sheet

Identity Theft Tip Sheet

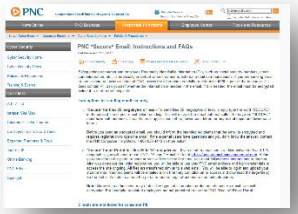
More policies

Your Commitment
Privacy Policy
Security Home Page
Security Policy / Tips
Get Help and Report
Additional Resources

Security – Policy and Tips

Don't Fall for a Phish

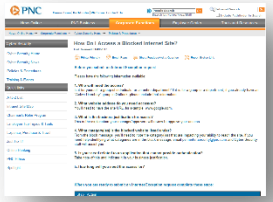
Email Encryption



When Apps Go Rogue

Contacting Your Third Party Management Office

Requesting Access to a Blocked Site

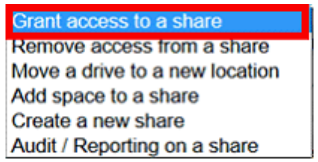


Requesting an Encrypted USB Device

Requesting a New Shared Folder on a Network Drive

Use the steps below to create a form requesting the folder and indicate who should have access.

1. Click to access ServiceNow.
2. Select Catalog ->User Access ->Shared Folder Access.
3. From within the request form select: "Grant access to a share" from the drop down menu.



Requesting a New SharePoint Site

1. Click to access the SharePoint Support Center.
2. Select **New Site** and answer the questions to set up the site.

Your Commitment
Privacy Policy
Security Home Page
Security Policy / Tips
Get Help and Report
Additional Resources

Privacy and Security – Get Help and Report

What should you do when customer data has been compromised or is suspected of being comprised?

You must complete a Security Incident Report (SIR) when the following have occurred:

- Information exposed contains at least one of the data elements that comprise Sensitive PII or General PII coupled with any sensitive personal information
- When it is possible that a customer's confidential data has been compromised by either PNC or our vendor partners

While most areas of the SIR have drop downs to lead you through the process, completing the Incident narrative section is very important; be as detailed as possible with the factual data.

What should you do when you suspect someone or something is attempting to get access to confidential information through PNC systems?

Send an email to: abuse@pnc.com for further investigation.

If an email looks suspicious to you:

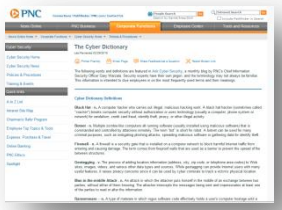
- Forward it to PNC Cyber Defense at abuse@pnc.com.
- Do not attempt to respond or click on any links, but do hold on to the message until you receive a response with specific instructions.
- If you do NOT receive a response, and it has been 72 hours or more since you submitted the message, you may safely process the message as you would routinely do.

Have a question? Where can you get help?

Call PNC Cyber Defense, 412-787-8765/8766, 24 hours a day, seven days a week.

Privacy and Security – Additional Resources

Cyber Dictionary



Privacy Center

AML Program - Your Commitment

To adhere to the AML Program:

- **Comply**: Know and apply the policies and procedures applicable to your role within your line of business.
- **Detect and Deter**: Watch for and recognize red flags of money laundering, terrorist financing and sanctions violations.
- **Report**: Use one of the appropriate methods to report suspicious activity.
- **Get support**: When needed.

AML Program - Reporting Suspicious Activity

When reporting suspicious activity:

DO:

at least <u>one</u> of the following to report the suspicious activity:

- File the **PNC online Security Incident Report (SIR) or its equivalent within your line of business** to document your observation and trigger an appropriate review by accessing **https://securityincidentreport.pnc.com** located on the PNC Intranet.
- If you do not have access to PNC Intranet, **report the suspicious activity directly to your manager**.
- Escalate the matter directly to Bank Secrecy Act (BSA) Anti-Money Laundering (AML) and Sanctions Compliance.
- Report the activity using the PNC Business Conduct and Ethics Hotline by calling 1-866-785-9753.

And discuss the incident internally with those who need to know.

DO NOT:

- Say or do anything that could directly or indirectly alert the customer or employee about your suspicions. Doing so is a serious violation of law. Referrals must remain strictly confidential.
- Investigate the matter on you own. PNC's investigators and compliance officers will let you know if you need to do anything further regarding the incident.
- Access the SIR link and practice completing a report.

Your Commitment
Policy and Procedure
Getting Help
Common Red Flags
Reporting Activity
Glossary

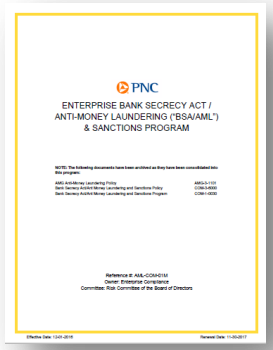
AML Program - Getting Help

Use the Policy and Procedure links in this guide or contact the PNC Business Conduct and Ethics Hotline by calling 1-866-785-9753.

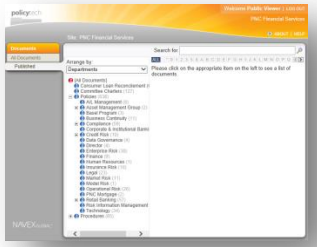
AML Program - Policy and Procedure

Click on the thumbnails below to access policy and procedure information for the AML Program.

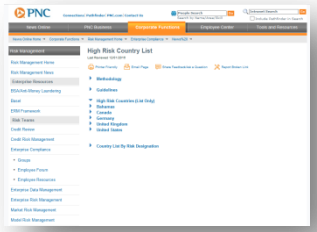
Enterprise BSA/AML & Sanctions Program



Policy Manager



High Risk Country List



Line of Business Specific Policy

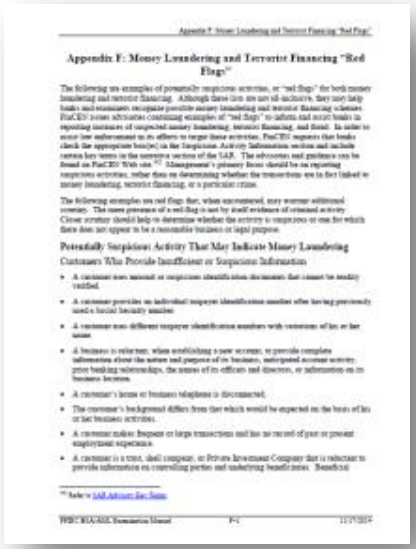
1. Click on Policy Manager. The home page of Policy Manager displays.
2. In the table of contents on the left side of the page, click to expand Procedure.
3. Locate and click on your line of business.

Your Commitment
Policy and Procedure
Getting Help
Common Red Flags
Reporting Activity
Glossary

AML Program – Common Red Flags

Suspicious transaction activity may be complex in nature, unusually large, follow an unusual pattern, or have no apparent economic or business purpose. Simply because a customer deviates from activity that is typically observed does not necessarily mean that the customer is engaged in criminal activity; however, lacking a reasonable explanation for the activity, further investigation is warranted.

Some red flags are listed below. To access a more complete list of red flags in the *FFIEC BSA/AML Examination Manual*, click on the thumbnail to the right and then click **Appendix F** from the table of contents.



Appendix F: Money Laundering and Terrorist Financing "Red Flags"

Potentially Suspicious Activity That May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer refuses or is reluctant to provide information or identification
- A customer provides minimal or vague information that you cannot readily verify or information that proves to be suspicious
- A customer uses a non-local address (e.g., a customer is located far from your office location but wants to open an account at your office)
- A customer refuses to proceed with or abruptly withdraws a transaction after learning a Currency Transaction Report (CTR) will be filed or that identity will be verified
- A customer opens an account where the source of funds is not readily apparent (example: a student opens an account with a large amount of cash)
- A customer whose transaction activity is across a series of accounts involving multiple cash deposits and withdrawals under the $10,000 reporting threshold (example: three $7,000 cash deposits on three consecutive days versus one single transaction of $21,000)
- A customer whose transaction activity or business terms that economically do not make sense, such as unique fund flows and excessive fees/revenue projections
- An employee who fails to conform to recognized policies, procedures and processes

Your Commitment
Policy and Procedure
Getting Help
Common Red Flags
Reporting Activity
Glossary

AML - Glossary

Documentary Verification	Documentary verification is the process of verifying a customer's identity by examining a document that includes customer identification information, such as a driver's license, to verify the information provided by the customer is correct.
Due Diligence	The steps that we take to achieve KYC. "Due diligence" is the level of diligence that is due, or called for, in the circumstances. It can include steps such as knowing the source of funds from a customer, identifying the beneficial owners of a customer that is a business or other entity, performing internet searches on those parties, and searching their names against negative news databases.
High Risk Customer (HRC)	Customers whose business, product, geographic, or other attributes indicate that they are a higher risk for money laundering, terrorist financing, or sanctions violations. Examples include private ATM owners/operators, casino owners/operators, marijuana related businesses, customers associated with certain foreign countries, etc. High risk customers require enhanced due diligence (EDD) at account opening and throughout the relationship.
Know Your Customer (KYC)	To acquire a solid understanding of the customer, its business or occupation and the type of legitimate activity that we can expect to see in the customer's accounts. Strong KYC provides a baseline that is essential in order to identify activity that is suspicious and might be evidence of fraud, money laundering, terrorist financing, sanctions violations, or other illicit activities.
Non-Documentary Verification	Non-documentary verification is the process of verifying a customer's identification information through sources such as contacting another bank that the customer provides as a reference, or accessing a credit bureau report and comparing the information provided by the customer with the credit bureau record.
OFAC List	OFAC publishes a list of organizations and individuals (specially designated nationals and blocked persons), with whom it is unlawful to do business. The owner of any account opened at PNC is reviewed against this list as well as other government lists to determine if the customer is a sanctioned person. This is usually done behind the scenes, systematically. Some lines of business do complete their own OFAC list checks. If PNC systems or any employee identifies an entity on the list, the sanctions rules can require PNC to reject, block or freeze transactions, accounts, funds and other assets.

More definitions

Your Commitment
Policy and Procedure
Getting Help
Common Red Flags
Reporting Activity
Glossary

AML - Glossary

Money Laundering

Money laundering is a three-stage process that involves the "washing" of "dirty money" with the objective of making it appear legitimate or "clean":

Dirty money – money obtained illegally such as from narcotics trafficking.

- **Placement stage** – dirty money is introduced into the financial system, undetected by law enforcement. (example: several cash deposits under the currency transaction reporting threshold of $10,000)
- **The layering stage** – once the money is "placed," a transaction or series of transactions are conducted with the purpose of creating "layers" between the money and its source, often involving a confusing or complicated paper trail. (example: numerous wires)
- **The integration stage** – using the dirty money to invest in or purchase legal assets, so as to make the money appear legitimate or clean. (example: purchase and resale of tangible assets such as inventory for a business, monetary instruments or real estate)

Apparently clean money – the outbound stream of money after the three stages are complete. The money appears to be clean, although it is not.

Sanctions Violations

Activities that violate laws against doing business with targeted foreign countries, terrorist-sponsoring organizations, international narcotics traffickers and other designated individuals and entities. The Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces US sanctions laws. All PNC employees, wherever located, must comply with these. PNC is also required to comply with non-US sanctions programs in other jurisdictions where it operates.

Senior Foreign Political Figure

A current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials; a senior official of a major foreign political party; and a senior executive of a foreign government-owned commercial enterprise. This definition also includes a corporation, business, or other entity formed by or for the benefit of such an individual. Senior executives are individuals with substantial authority over policy, operations or the use of government-owned resources.

Also included in the definition of a senior foreign political figure are immediate family members of such individuals, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure.

More definitions

Your Commitment
Policy and Procedure
Getting Help
Common Red Flags
Reporting Activity
Glossary

AML - Glossary

Suspicious Activity	Any unusual or unexplained activity or transaction that is not consistent with normal or expected business or banking activities of customers, employees and vendors. If the characteristics of an event do not appear to be "normal" or you have difficulty understanding why a customer or employee is engaging in a particular activity or transaction, do not try to investigate the case yourself. Instead use the steps under *Reporting Activity* to report the details.
Terrorist Financing	Terrorist financing includes providing money to fund specific terrorist activities, to develop and support a terrorist organization, or to sustain an individual terrorist on a day-to-day basis. While terrorist financing may involve some elements of money laundering, its focus is actually quite different. As opposed to traditional money laundering, which involves the disguising of criminal proceeds as legitimate funds, terrorist financing involves the disguising of the use of (potentially legitimate) funds for terrorist activities. For this reason it is often referred to as "reverse money laundering." Terrorist financing also includes unique characteristics. For example, it can be carried out in smaller dollar amounts than money laundering, and involve products and services that are not commonly used for money laundering (example: prepaid cards vs. wire transfers). It is also more likely to involve the use of nonprofit or charitable organizations.