DISTRIBUTION PARTNER OPERATIONS MANUAL
For Resellers of Business Funded Closed Loop U.S. Dollar Products (HAWK Commerce)

Effective July 1st, 2018
Version 1.1

Document Version Control

Version	Date	Author	Change Description
1.0	6/1/2017	Ryan Schmitz	Initial Version of Distribution Partner Operations Manual
1.1	7/1/2018	Ryan Schmitz	Minor Edits

To Our Valued Distribution Partners:

Thank you for choosing to join HAWK Commerce as a Distribution Partner.

Among the tools used by the United States government in the fight against money laundering and terrorist financing is the Bank Secrecy Act or "BSA." The USA PATRIOT Act of 2001 was signed into law in response to the September 11th terrorist attacks as the United States and other concerned countries began to recognize the link between money laundering and global terrorism. The USA PATRIOT[1] Act made it mandatory for all money services businesses ("MSBs") and their distribution partners to have an effective Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) compliance program. Each Program must be commensurate with the risks posed by the location, size, nature and volume of the services provided by the MSB.

Blackhawk Network Holdings, Inc. and its subsidiaries (together "Blackhawk Network") are committed to conducting business in accordance with all applicable laws, rules, and regulations, including the BSA and USA PATRIOT Act. Blackhawk Network is committed to actively preventing money laundering and any activity that facilitates money laundering, criminal activity or the funding of terrorists.

By providing this manual to its Distribution Partners, HAWK Commerce shares an overview of the BSA AML/CTF regulatory requirements and sets expectations for how its distribution partners should operate a successful program within its network while supporting the collective goal of compliance with all applicable laws and regulations. The manual also contains useful guidelines for establishing your own risk-based AML programs and best practices for the sale of prepaid access products. The information is not, however, legal advice, and does not attempt to address all BSA or other legal requirements that may apply to your business. For official guidance, we urge you to visit the U.S. Treasury website dedicated to BSA and AML issues: www.fincen.gov. If you have questions about how these laws apply to your business, you should consult with your own legal advisor.

It is important to understand that failure to comply with the BSA or AML/CTF laws and regulations can result in substantial civil and criminal fines, forfeitures, and imprisonment. In addition, failure to comply with the laws may also result in termination of your status as a HAWK Commerce Distribution Partner.

Please note the capitalized terms within this document are defined in Appendix A. Contact HAWK Commerce if you have questions about how these requirements apply to the HAWK Commerce products and services you offer.

Thank you for your commitment and support in the fight against money laundering and terrorist financing.

HAWK Commerce Compliance Team

[1] The USA PATRIOT Act is an Act of Congress that was signed into law on October 26, 2001. The title of the act is a ten-letter backronym (USA PATRIOT) that stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

TABLE OF CONTENTS

1 BACKGROUND AND IMPLICATIONS OF ANTI-MONEY LAUNDERING REGULATIONS

The federal government, through the Financial Crimes Enforcement Network (FinCEN), a bureau within the Treasury Department, issues written regulations with the primary goal of identifying and preventing money laundering. The basic framework for anti-money laundering (AML) obligations imposed on financial institutions was established by Congress in the Bank Secrecy Act (BSA), initially adopted in 1970. FinCEN has issued regulations requiring financial institutions, including money services businesses, to keep records and file reports on financial transactions that may be useful in the investigation and prosecution of money laundering and other financial crimes. Additionally, the BSA has been broadened by the USA PATRIOT Act of 2001, which was enacted in reaction to terrorist acts on the United States.

1.1 Description of Money Laundering and Terrorist Financing

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money. Through money laundering, the criminal attempts to transform monetary proceeds derived from criminal activity into funds with an apparently legal source (turning "dirty" money into "clean" money). If illegally obtained money is successfully laundered, criminals maintain control over their illegally obtained funds and can use them in the nation's legitimate financial systems.

Money laundering typically occurs in three stages: Placement, Layering, and Integration.

- **Placement** is the introduction of the illegal proceeds into the financial system. This is the most vulnerable step with regards to detection in the "washing" cycle for criminals. Many of them are familiar with the dollar thresholds that trigger recordkeeping and reporting, so they attempt to work around the requirements and remain anonymous. Two methods they often use are structuring and smurfing. **Structuring** is breaking up a potentially large, reportable transaction into several smaller transactions to avoid triggering recordkeeping or reporting requirements for the person(s) conducting the transaction. **Smurfing** is breaking up a large sum of money and distributing it to several people who each place a transaction that doesn't trigger any reporting requirements.
- **Layering** involves moving funds around in an attempt to camouflage the source and ownership of the funds.
- **Integration** is the final stage, where "clean" funds are placed back into the economy to create the perception of legitimacy. This can be done through the purchase of cars, businesses, real estate, or other assets.

Money laundering is not limited to cash. Money laundering can be done through any type of financial transaction, including, but not limited to, funds transfers, money orders, checks, debit cards, prepaid products such as stored value cards and other forms of prepaid access, and credit card transactions.

AML laws apply to any funds derived from illegal activities, such as funds held by human smugglers, drug traffickers, terrorists, organized crime, tax evaders and other groups and individuals seeking to transfer, spend and/or invest money gained from any type of crime.

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity. Terrorists and terrorist organizations derive income from a variety of sources, often combining both lawful and unlawful funding. The terrorist financer will want to disguise the illegal destination of the funds, while trying to maximize the revenues for the sponsored organization. The need to camouflage the nature, location, source, ownership, or control of the funds means that terrorist financing has certain similarities with traditional money laundering, namely the use of the three stages to place, layer and integrate the funds in the international financial system. The crucial difference between traditional money laundering and terrorist financing is that traditional money

laundering is focused on converting illegally obtained funds, whereas terrorist financing is focused on using funds (whether or not illegally obtained or involving proceeds of criminal conduct) to facilitate criminal activity.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. For the purposes of this document, the policies, procedures, and controls identified for AML also apply to counter-terrorist financing (CTF).

1.2 AML Implications for HAWK Commerce and its Distribution Partners

HAWK Commerce's business involves prepaid access products that have been identified by FinCEN as a possible vehicle for money laundering and terrorist financing activities. Even though HAWK Commerce is not a bank, as a non-bank financial institution, it is subject to certain aspects of the USA PATRIOT Act, including the establishment of an AML program reasonably designed to detect and prevent money laundering and terrorist financing, and the implementation of sufficient controls to ensure that its Distribution Partners operate in line with HAWK Commerce's AML Program and the rules and regulations of the BSA.

All sales of prepaid access must be in accordance with HAWK Commerce's written policies and procedures provided herein and must comply with all applicable federal and state laws, rules, and regulations.

2 GENERAL POLICIES AND PROCEDURES

2.1 Distribution Partner Agreement

A HAWK Commerce Distribution Partner must:

- Only resell HAWK Commerce prepaid access products to other business entities. Resale to consumers is not allowed.
- Implement policies and procedures to verify the identity of the Distribution Partner's business client, if the business client purchases over $10,000/day in prepaid access products (closed loop products or open loop products or a combination of both).
- Implement a record retention policy requiring all payment and identifying information (regarding the Distribution Partner's business client) to be maintained, preserved and made available for inspection for five years after the date of sale of the prepaid access products.
- Establish a process for reporting suspicious activity to HAWK Commerce.
- Acknowledge and agree to prohibit cash payments for funding.
- Not sell prepaid access products to business clients that intend to further resell the products, without permission from HAWK Commerce.

It is the Distribution Partner's responsibility to put in place business policies and procedures to support these requirements.

2.2 Additional Requirements for All Distribution Partners

This section reviews additional requirements for all HAWK Commerce Distribution Partners. These requirements will assist in reducing the risk of fraud and money laundering utilizing HAWK Commerce prepaid access products.

2.3 Know Your Customer

Knowing your customers is one of the most effective weapons against money laundering and other financial crimes. All Distribution Partners must research and verify that each of their clients funding a prepaid access program is a valid legal business entity.

2.3.1 Sales of Prepaid Access to Business Clients

At a minimum, all Distribution Partners must obtain and record the following information for the business client *originating* the funding for the prepaid access program. Generally, the Distribution Partner's business client *originates* the funding for their prepaid access programs.

- Transaction date and time
- Business Name of Distribution Partner's business client
- Principal business client address (not P. O. Box)
- Business client telephone number (including area code)
- Business client Federal Tax ID (EIN/TIN)
- Business client contact name
- Number and denomination of prepaid access purchased
- Payment type sent to Distribution Partner (check, wire, ACH, credit card). Cash is not an approved payment type.
- Total amount purchased

- Description of how cards will be used (e.g., promotions, employee incentives)

Upon Hawk Commerce's request, Distribution Partners are required to release this business information to HAWK Commerce regarding their business client that *originates* the funding for each prepaid product order placed by the Distribution Partner.

2.4 Unusual or Suspicious Activity

One key goal of an AML program is identifying, recording, and reporting suspicious transactions or activity. There is no clear-cut definition of suspicious activity. What may appear or seem suspicious for one business client may be normal and appropriate for another. That is why, to the extent possible, it is important for you to know your business clients in order to be familiar with their normal use of your financial products. In addition, appropriate policies, procedures, and processes should be in place to monitor and identify unusual or suspicious activity. The level and sophistication of your monitoring program should be commensurate with the perceived risks for your business.

Even though suspicious activity as it relates to prepaid access products can be difficult to identify, there are certain activities called "red flags" that may suggest the presence of suspicious activity and should be investigated further.

2.4.1 Suspicious Activity "Red Flags"

The following are some of the "red flags" that suggest suspicious activity and may indicate that a business client is trying to use the purchase of prepaid access products to engage in a financial crime or fraud:

- A business client requests a prepaid access program for its employees. During the KYC due diligence process, verifying the business client's information is difficult, unavailable, unusual or inconsistent with other similar businesses. The business client may be a "front" or "shell" company.
- A business client asks that funding from returned prepaid access products be refunded back to them via a payment method or bank account *different* than the original source of funding.
- The payment source for funding a business client's prepaid access program is provided by an unexpected separate entity, not associated with the business client.
- A business client uses different tax identification numbers with variations of name.
- A business client is reluctant to provide complete information regarding: the type of business, the purpose of the program, or any other information requested, including Tax ID # or parent company information.
- A business client that offers bribes, tips or attempts to coerce a Distribution Partner's representative not to file any required recordkeeping or reporting forms.
- An existing prepaid access program for a business client suddenly changes or significantly changes over time without an apparent explanation. Examples could include increased funding for some or all employees, the number of employees increase to an unexpected level based on what is known about the client.
- Unexpected changes in frequency and / or amount of repeat "bulk" prepaid access purchases by a business client.
- A business client or contact alters the spelling or order of his / her name when ordering.
- A business client wants to void an order once identification is requested.

Whether you determine that the activity is suspicious or not must be based on all the facts and circumstances relating to the transaction and the business client in question. Different situations will require different conclusions. In some cases, the facts of the situation may clearly indicate the

need to report what you observed. In other cases, more thought will be needed to determine whether a transaction is indeed suspicious under applicable laws and regulations.

It is very important that you do not inform the business client that you think his or her behavior is suspicious. Information regarding the reporting of suspicious activity is highly confidential, and disclosing it carries severe federal penalties which are actively enforced. The information in the wrong hands could potentially compromise a law enforcement investigation. To minimize the risks of an inadvertent disclosure, information for the suspicious activity report should only be shared with HAWK Commerce and internally only on a need-to-know basis.

2.5 What You Must Do When You Encounter Suspicious Activity

Distribution Partners must not complete any transaction that is deemed to be suspicious, and must take steps to report it to HAWK Commerce right away.

Reporting of suspicious activity is one of the primary requirements of the BSA. It is critical to law enforcement efforts to combat terrorism and terrorist financing, money laundering, and other financial crimes.

2.5.1 Suspicious Activity Reports (SARs)

The following are the regulatory requirements for Suspicious Activity Reports, or SARs:

- SARs are required by the federal government for any transaction, or pattern of transactions, that is attempted or completed and involving at least $2,000, when the Distribution Partner knows, or has reason to suspect, that the activity:
    - Involves funds derived from an illegal activity or is intended to hide funds derived from an illegal activity
    - Is structured to avoid record keeping or reporting requirements
    - Has no business or apparent lawful purpose
    - The business client is providing false or expired information
- Suspicious transactions totaling less than $2,000 may be reported at your discretion.
- A SAR must be filed no later than 30 days after the date of detection. If no suspect can be identified, the period for filing is extended to 60 calendar days. The time period for filing a SAR starts when you know or have reason to suspect that the activity meets one or more of the definitions of suspicious activity.

SARs are confidential documents. Never tell a business client that a SAR has been or may be filed. It is illegal to tell any person involved in a suspicious transaction that a SAR has been or may be filed.

2.5.2 Suspicious Activity Reporting by Distribution Partners

Distribution Partners are required to send the suspicious activity information to HAWK Commerce right away for review and processing.

- To submit suspicious activity information to HAWK Commerce for review and processing, send any and all relevant information regarding the suspicious activity to HAWK Commerce's Risk Department at Investigations@bhnetwork.com.
    - You must send this information to HAWK Commerce within 48 hours of the suspicious activity being detected.
    - HAWK Commerce will review the information and then will decide at HAWK Commerce's own discretion whether or not the activity warrants the filing of a SAR.

- HAWK Commerce will not disclose to you whether or not a SAR has been filed based on the information you provided.

2.5.3 Unusual Activity

There are times when you may notice questionable or unusual activity in your place of operation. Please note that unusual activity may not necessarily be suspicious activity and you must investigate and assess such occurrences before reporting them as suspicious.

The time period for reporting unusual activity starts when the unusual activity is deemed suspicious. In all cases, the review of the transaction(s) or account should be done as quickly as possible to assist HAWK Commerce and law enforcement.

2.6 SAR Recordkeeping and Safe Harbor Requirements

2.6.1 Recordkeeping

All records related to SARs, including the filed forms, will be centralized and stored at HAWK Commerce for a period of at least five (5) years from the date of creation.

2.6.2 Safe Harbor Provisions

The safe harbor provisions in the BSA provide protection from civil liability to your business and employees for all suspicious activity reporting. Federal law will protect any person that reports suspicious activity as long as good faith is demonstrated (i.e. the person reporting the activity truly believes a transaction is suspicious and provides the information honestly).

If a Distribution Partner does not report suspicious activity due to "willful blindness," there may be liability incurred by the Distribution Partner. "Willful blindness" is when someone has the knowledge of a reportable activity but intentionally does not report it. If you locate or later remember a transaction that was not reported, please make every effort to report it because a late report is better than not reporting at all.

2.7 Currency Transaction Reporting

The BSA requires the reporting of any cash transactions of more than $10,000 (that is, anything $10,000.01 and over) made in any one day by any person or on behalf of another person. Since Currency Transaction Reports (CTRs) track large financial transactions, they create a paper trail for transactions that would otherwise be invisible. The filing of CTRs mitigates the risk of criminals hiding large transactions of illegal proceeds by conducting the transactions in cash.

Distribution Partners are not permitted to accept cash as a form of payment for funding prepaid access programs at HAWK Commerce, and therefore the filing of CTRs will not apply to HAWK Commerce Distribution Partners.

3 ON-GOING AGENT OVERSIGHT

Inherent risks are associated with the distribution of prepaid access products through third party Distribution Partners. Risks include those associated with the underlying nature of the prepaid access product being sold or with the prepaid access transaction itself. Other potential risks arise from, or are increased by, the involvement of a particular third party, possibly due to reputational, financial, or legal factors. Failure to manage these risks could expose HAWK Commerce and its Distribution Partners to regulatory action, financial loss, litigation and reputational damage, and may even impair their ability to establish new or service existing customer relationships.

HAWK Commerce is required to demonstrate additional oversight of its Distribution Partners with the following requirements.

3.1 Keeping Your Information Current with HAWK Commerce

As part of HAWK Commerce's regulatory obligations, HAWK Commerce frequently must provide information to certain parties about its Distribution Partners that are authorized to sell HAWK Commerce products. To meet this requirement, you must notify HAWK Commerce when significant changes to your business occur. We recommend that you send this information as soon as possible after the changes occur or within thirty (30) calendar days at the latest.

3.1.1 Updated List of Business Locations

Distribution Partners must keep their list of business locations current with HAWK Commerce. Key data elements that must be maintained include:

- Distribution Partner's legal name
- Business locations including: address, city, state, zip code (no P.O. Box allowed)
- Telephone numbers
- Distribution Partner contacts

3.2 Legal Requests

3.2.1 Responding to Law Enforcement Requests

Law enforcement agencies may request information and records, as part of an investigation. Employees must direct all such requests to a manager or the internal legal department trained to handle such requests.

The Distribution Partner must cooperate with requests from law enforcement agencies: however, the Distribution Partner must not release accountholder or business client information without first receiving proper summons, subpoena or court order. This is necessary to ensure compliance with customer and accountholder privacy laws.

The Distribution Partner must notify HAWK Commerce's Risk Department by emailing Investigations@bhnetwork.com promptly if there is any request from a law enforcement agency involving HAWK Commerce prepaid access products.

3.3 Working with HAWK Commerce Compliance Team

From time to time, HAWK Commerce Compliance may contact the Distribution Partner to:

- Request documentation or request enhancements to existing documentation.
- Obtain missing information
- Obtain information to support a request from law enforcement involving one of your business locations

- Provide regulatory updates
- Alert you to suspicious activity or unusually high volume from one of your locations identified through HAWK Commerce's monitoring program

3.4 Remediating Deficiencies

HAWK Commerce's on-going Distribution Partner oversight activities include periodic reviews to make sure the Distribution Partner is compliant with applicable laws and regulations and with our operating principles. HAWK Commerce will contact the Distribution Partner if areas that need attention or correction are identified.

Depending on the circumstances, remediation and correction efforts may include:

- Reviewing your business policy and procedures for compliance
- Requiring remediation of the problem within a defined timeframe
- Training or re-training your function critical employees

Certain or repeated violations of laws and regulations may result in termination of your Distribution Partner status.

4 APPENDICES

Appendix A – Summary of Terms

Appendix B – HAWK Commerce Risk and Compliance Contacts

Appendix A – Summary of Terms

Term	Definition
Anti-Money Laundering (AML)	The comprehensive efforts by government, law enforcement, and businesses to detect, report, and prevent money laundering activities.
Distribution Partner	Distribution Partners are approved to resell or market HAWK Commerce products.
Bank Secrecy Act (BSA)	U.S. government legislation that was created in 1970 to prevent financial businesses from being used as tools by criminals to hide or transfer money derived from their illegal activity. This includes requiring financial institutions to report cash transactions in excess of $10,000 and to provide documentation on suspicious activity.
Accountholder	The owner or user of the prepaid access product.
Closed Loop Gift Products	These are *exempt* merchant-specific gift cards at HAWK Commerce, which can only be redeemed with that merchant. This also includes affiliated merchant cards or limited scope cards, such as mall cards and mass transit cards.
Content Provider	The prepaid access Content Provider is the bank, MSB, or other entity that issues prepaid access products.
Currency Transaction Report (CTR)	A form that financial businesses are required to file when any currency transaction of more than $10,000 is made in any one day by any person or made on behalf of another person. This report is required by the BSA and is not a confidential document.
Customer Identification Program (CIP)	A company's formal customer identification and verification policies and procedures.
Financial Crimes Enforcement Network (FinCEN)	A bureau of the U.S. Department of the Treasury that collects and analyzes information about financial transactions in order to combat money laundering, terrorist financing, and other financial crimes.
FinCEN Prepaid Access Rule	On July 26, 2011, FinCEN issued a final rule ("the FinCEN rule") amending the BSA regulations and establishing comprehensive regulatory requirements for sales of prepaid cards and other prepaid access.
High Intensity Drug Trafficking Area (HIDTA)	Certain parts of the United States determined to be critical drug-trafficking regions.
High Intensity Financial Crime Area (HIFCA)	Certain parts of the United States that have been jointly designated by the U.S. Treasury and Justice Departments as having a high risk for money laundering and other financial crimes.
Integration	The last of the three stages of money laundering where "clean" funds are placed back into the economy to create the perception of legitimacy. This can be done through the purchase of cars, businesses, real estate, or other assets.

Term	Definition
Issuer	An entity, which is typically a bank or MSB, that issues prepaid access to a cardholder. Also called the issuing bank. The Issuer must be authorized by a Payment Network (e.g. Visa or MasterCard) to operate a prepaid access program. For prepaid access bearing the brand of American Express, the prepaid access is issued directly by American Express. For prepaid access bearing the brand of Discover, the prepaid access may be issued directly by Discover, or by a bank or MSB authorized by Discover.
Know Your Customer (KYC)	Refers to the concept of identifying your customer and understanding their expected transactions. A Customer Identification Program (CIP) is a type of KYC program.
Layering	The second of the three stages of money laundering that involves moving funds around in an attempt to camouflage the source and ownership of the funds.
Money Laundering	The attempt to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. Through money laundering, the criminal attempts to transform monetary proceeds derived from criminal activity into funds with an apparently legal source (turning “dirty” money into “clean” money). If illegally obtained money is successfully laundered, criminals maintain control over their illegally obtained funds that they’ve introduced into legitimate financial systems. Money laundering is not limited to cash. Money laundering can be done through any type of financial transaction, including, but not limited to, funds transfers, money orders, checks, debit cards, prepaid products such as stored value cards and other forms of prepaid access, and credit card transactions. AML laws apply to any funds derived from illegal activities, such as funds held by human smugglers, drug traffickers, terrorists, organized crime, tax evaders, and other groups and individuals seeking to transfer, spend, and/or invest money derived from any type of crime.
Money Services Business (MSB)	A business is classified as an MSB if it: is a provider or seller of prepaid access; is an issuer, seller, or redeemer of money orders and/or traveler’s checks; offers check cashing, currency dealing, or exchange; AND conducts more than $1,000 in money services business activity with the same person, in one type of activity, on the same day; OR provides money transmission services in any amount.

Term	Definition
Office of Foreign Assets Control (OFAC)	A department of the U.S. Treasury that enforces economic and trade sanctions against countries and groups of individuals involved in terrorism, narcotics, and other disreputable activities.
Open Loop Gift Products	These *exempt* gift cards at HAWK Commerce can be used for purchases at multiple, unaffiliated merchants connected to a payment network (e.g., AMEX or Discover). .
Placement	The first of the three stages of money laundering that allows the introduction of illegal proceeds into the financial system. This is the riskiest step in the "laundering" cycle for criminals, as it's the most vulnerable to detection. Many of them are familiar with the dollar thresholds that trigger recordkeeping and reporting so they attempt to work around the requirements to remain anonymous.
Prepaid Access	Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number. Prepaid access includes prepaid products, open loop gift products and closed loop gift products. Previously referred to as "Stored Value."
Safe Harbor	A provision in the laws requiring suspicious activity reporting that provides protection from civil liability for anyone involved in preparing and filing the report, as long as the report was filed in good faith.
Smurfing	One of the methods used by money launderers at the placement stage by breaking up a large sum of money and distributing it to several people, who each initiate a transaction that does not trigger any reporting requirements.
Structuring	One of the methods used by money launderers at the placement stage by breaking up a potentially large, reportable transaction into several smaller transactions to avoid triggering recordkeeping or reporting requirements and retain the anonymity of the person(s) conducting the transaction.
Suspicious Activity Report (SAR)	A highly confidential form required by the Bank Secrecy Act, used to report suspicious activity and known or suspected violations of law. It is used by law enforcement for investigations of money laundering, terrorist financing, or other criminal cases. Revealing that a person may be reported or has been reported on a SAR carries severe federal penalties.

Term	Definition
Terrorist Financing	The processing of funds to sponsor or facilitate terrorist activity. Terrorists and terrorist organizations derive income from a variety of sources, often combining both lawful and unlawful funding. The terrorist financier will want to disguise the illegal end of the funds, while trying to maximize the revenues for the organization sponsored. The need to camouflage the source of the funds means that terrorist financing has certain similarities with traditional money laundering, namely the use of the three stages to place, layer, and integrate the funds in the international financial system. The crucial difference between traditional money laundering and terrorist financing, both of which involve concealing or disguising the nature, location, source, ownership, or control of money, is that traditional money laundering is focused on converting illegally obtained funds, while terrorist financing is focused on using funds (whether or not illegally obtained or involving proceeds of criminal conduct) to facilitate criminal activity. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Policies, procedures, and controls identified for AML typically apply to counter-terrorist financing (CTF).
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. An act of Congress that was signed into law in 2001 after the September 11th attacks, and instituted changes to a broad range of laws. For financial institutions, it strengthened existing U.S. measures and added new laws to prevent, detect, and prosecute money laundering and terrorist financing.
Willful Blindness	The practice of intentionally turning a blind eye to red flags or other circumstances that should prompt a reasonable person to question the activity. Courts have held that an individual cannot avoid liability by intentionally remaining ignorant of facts that they should have ascertained.

Appendix B– HAWK Commerce Risk and Compliance Contacts

1. **HAWK Commerce Compliance Department:**

   Email: Fenton.compliancequestions@bhnetwork.com

2. **HAWK Commerce Risk Department:**

   Email: Investigations@bhnetwork.com