FRAUD FIGHTER™
by UVeritech

WHITEPAPER

BEST PRACTICES IN RETAIL: COUNTERFEIT FRAUD & ID THEFT PREVENTION

Designing a “multi-layered” program
to prevent in-store transaction fraud and
comply with regulatory I.D. verification requirements.

Sean Trundy,
COO

1743 S. Grand Ave., Glendora, CA 91740 | 800.883.8822 | info@fraudfighter.com

Table of Contents

INTRODUCTION

Businesses are susceptible to a tremendous degree of fraud in their store or branch locations. Organizations that operate physical store locations are faced with a complex range of vulnerabilities through which both the casual and sophisticated criminal are able to strike. Fraud loss totals in North America number in the hundreds of billions of dollars every year. Counterfeit fraud and ID theft account for the lion's share of these losses.

Coupled to this is a convergence of obligations that businesses of all sizes have to comply with Federal, State and/or Local legislative guidelines regarding the need to verify identification documents at the specific points in time certain transactions are conducted, and further, to maintain and safeguard records related to such I.D. verifications.

Facing such a confusing array of vulnerabilities exposes companies to fraud liability. This liability arises not only from the direct "hard dollar" losses experienced anytime a fraudulent event occurs, but also from the fines and other punitive measures that may be faced by the company should regulatory procedures not be followed. In addition, failure to adequately create policies and procedures to mitigate against such vulnerabilities and to perform according to legal guidelines may lead to frequent, costly audits and investigations by any number of local, state or federal government agencies.

The Keys to Success

Key to addressing such a broad exposure to fraud and potential regulatory violations is the ability to structure an intelligently designed solution incorporating successive "layers" of document validation. Just as valuable computer networks require, first, a firewall, next, anti-spyware, anti-malware, intrusion detection and virus scanning solutions, so must the critical transaction process be secured with POS-level validation, coupled with manager level advanced validation, ID authentication, and document image capture and storage capabilities.

To employ the appropriate company or government specific antifraud and compliance program with the right security layers begins by management gaining a greater understanding of the types of fraud risks that can undermine their business objectives.

TRANSACTIONAL FRAUD

TYPES AND PREVALENCE OF TRANSACTION FRAUD

Counterfeit Currency

Official currency counterfeiting statistics are difficult to come by. According to the U.S. Secret Service, in the U.S., there was approximately $200 Million of counterfeit currency circulating in 2009. This number has been steadily rising, with one report showing that counterfeit currency activity in the U.S. increased by 69% from 2003 through 2006.

Reasons for the extreme growth in the volume of counterfeit money are simple. In years past, production of quality counterfeit currency required the skills of a journeyman artist to engrave plates and manage the inherent challenges of offset printing. Today, however, graphics software and high-quality, low cost color printers mean the rank amateur can produce passable counterfeit notes.

Fake Negotiable Instruments

Checks and money orders — including U.S. Postal money orders — are commonly counterfeited these days. In the United States, the number of Federal Deposit Insurance Corporation Special Alerts on counterfeit checks, bank drafts, and money orders has increased dramatically in recent years – with more than a 500 percent increase in alerts in less than four years. The FBI has cited "the pervasiveness of check fraud and counterfeit negotiable instrument schemes" as a leading factor in the growth in external bank fraud, which has "replaced bank insider abuse as the dominant [financial institution fraud] problem confronting financial institutions."[1] In 2007, the U.S., Canada, and other countries jointly intercepted more than 590,000 counterfeit checks with a total face value of approximately $12.2 billion.

However, it doesn't stop there. Forgers have learned that a high quality color printer, digital scanner, and a graphics editing program, such as PhotoShop, enable them to make credible reproductions of just about any type of "secured" negotiable instrument. Thus, businesses accepting traveler checks or gift checks from any of the major branded companies (American Express, Thomas Cooke, Visa, MasterCard, etc.) are susceptible to fraud. Additionally, other traditionally "safe" instruments, such as Official Checks (issued by a bank – e.g. money orders and cashiers checks) as well as government checks, such as welfare, unemployment and tax returns, are just as likely to be counterfeit as any of the previously mentioned types of "secured" financial instrument.

[1] U.S. Dept of Justice Public Advisory: Special Report on COUNTERFEIT CHECKS AND MONEY ORDERS

Merchandise Return / Return Receipt Fraud

Return Receipt fraud is one of the leading causes of fraud loss in the retail industry.

According to the National Retail Federation's annual Return Fraud Survey, completed by loss prevention executives at 134 retail companies, two-thirds of retailers (69%) say their company's return policy has changed in the past to account for fraud. However, the losses remain staggering: the retail industry lost an estimated $2.7 billion in return fraud during the 2009 holiday season, and an estimated $9.6 billion for the year.

According to the survey, 93.1% of retailers said stolen merchandise has been returned to their stores in 2009, up from 88.9 percent in 2008. In addition, three-quarters of retailers (75.4%) say they have experienced returns of merchandise purchased with fraudulent or stolen tender while 43.1 percent say they have experienced returns using counterfeit receipts.

Identity Fraud

Identity fraud is a crime in which an impostor obtains key pieces of personal identifying information, such as Social Security numbers and driver's license numbers, and uses them for their own personal gain. A 2009 study conducted by Javelin Strategy, titled "The LexisNexis® True Cost of Fraud Study" indicated that U.S. businesses lose nearly $100 Billion annually from fraud, of which nearly half, or $48 Billion, stems from ID related fraud. The 2010 Identity Fraud Survey Report also released by Javelin Strategy & Research in February of 2010 found that the number of identity fraud victims in the United States increased 12 percent year-over-year, to 11.1 million adults in 2009, while the total ID fraud amount increased by 12.5 percent to $54 billion.

Overall ID fraud is on the rise, with certain merchant types being targeted more than others. With the economic downturn and increasing sophistication in criminal fraud methods (particularly the underground industry for compromised card information) identity fraud has been trending upward for the last several years.

The Cost of Fraud

- **$200 million** in counterfeit currency in the U.S. (2009 US Treasury) $103M confiscated in 2009 by Secret Service
- **$12.2 billion** in losses due to check fraud (2006 American Bankers Association)
- **$500 million** per year in credit card fraud
- **$31 billion** in US existing account fraud (2009 Javelin Strategy and Research)
- **$221 billion** worldwide per year due to identity theft (Aberdeen Group)

Generally speaking, all businesses are exposed to fraud resulting from thieves attempting to use another's financial identity via credit cards, check books, traveler checks, money orders, etc. Some businesses may have even greater exposure. Highly-exposed organizations can be loosely defined as those companies that provide access to some benefit as the result of the presentation of an ID document. The ability to access a personal account or credit line, creation of new accounts (e.g. – municipal utility,

financial, cell phone, etc.), vehicle rentals or in-store credit, are a few examples of this type of exposure.

Much of the above business activity may trigger COMPLIANCE issues associated with state and federal laws requiring the logging and verification of identity when conducting certain types of regulated transactions.

Types of I.D. Fraud Activity

Credit Card Fraud

Credit card fraud is a general term used to describe theft and fraud committed using a credit card or any similar payment mechanism (e.g. – debit card, gift card) as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. According to the Federal Trade Commission, while identity theft had been holding steady for the last few years, it saw a 21 percent increase in 2008. The costs of card fraud in 2006 were 7 cents per 100 dollars worth of transactions (7 basis points), and "total fraud costs in the U.S. broadly related to credit cards alone is conservatively estimated to exceed $16 billion annually[2]".

Phone or utilities fraud

Thieves may open a new phone or wireless account in the victim's name, or run up charges on their existing accounts. Thieves may use the victim's name to get utility services like electricity, heating, or cable TV.

"Account" Fraud

This type of identity fraud occurs when an identity thief misuses an existing bank, credit union, trading, retirement or other account of a victim. Account fraud refers to those cases where a person accesses some type of benefit, such as a membership or a deposit account, under the guise of false identification.

Bank/finance fraud

* Creating counterfeit checks using a stolen name or account number.
* Opening bank accounts in the victim's name and writing bad checks.
* Cloning the victim's ATM or debit card and making electronic withdrawals under their name.
* Taking out a loan in the victim's name.

Government documents fraud

* Getting a driver's license or official ID card issued in the victim's name but with their picture.
* Using the victim's name and Social Security number to get government benefits.
* Filing a fraudulent tax returns using stolen identification to receive fraudulent tax returns.

[2] Mercator Advisory Group, Inc. "Credit Card Issuer Fraud Management" Dec 2008

Other fraud

* Using fraudulent Social Security card under victim's name to get a job
* Renting a house or getting medical services with stolen ID.
* Giving stolen identity information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued under the victim's name.

Age Restricted Sales

Stolen and/or fake identity is commonly used by underage drinkers and smokers for the purchase of alcohol and tobacco products. Such underage sales expose the retailer to steep penalties.

Controlled Substance Sales

Stolen and/or counterfeit identity is one of the leading methods used by criminals to illegally obtain access to Class I prescription narcotics and the chemicals used in the production of Methamphetamine. Both of these activities are strictly regulated under federal law and require identity verification and recording at the time of purchase. A person's stolen ID may be use in connection with such purchases, and thus, may create complex legal issues defending themselves against prosecution for behavior they had no involvement with.

COST OF TRANSACTION FRAUD

Hard Costs

The "hard cost" of fraud refers to the actual dollar amount lost due to direct fraud activity. For example, when a bank receives a counterfeit $50 from a teller deposit customer, the hard-cost of the loss realized by the bank from the event is equal to $50.

Each type of business has its own unique mix or fraud exposure profile, with some trending towards credit card fraud, while others are more exposed to Identity Fraud, fraudulent checks and currency.

Annually, merchants pay $100 billion in fraud losses due to unauthorized transactions and fees/interest associated with charge-backs[3]. Counterfeit currency seizures in the United States totaled over $100 million in 2009. In 2007, the U.S., and Canada jointly intercepted more than 590,000 counterfeit checks with a total face value of approximately $2.3 billion[4].

Soft Costs

The "soft cost" of fraud refers to the expenses incurred by an organization as the result of a fraud event, exclusive of the actual "hard cost". For example, the controller's office may uncover a bank deposit discrepancy and must file and perform an audit report. The

[3] Calculated using data from 2009 LexisNexis Merchant Survey and 2006 U.S. Economic Census Bureau.

[4] U.S. Dept of Justice Public Advisory: Special Report on COUNTERFEIT CHECKS AND MONEY ORDERS

store manager where the event occurred must follow-up with a review and response to the audit, then these opportunity costs associated with lost work time continue as loss prevention will need to investigate by going on-site and interviewing involved parties, etc.

In addition, many fraud events, such as receipt of counterfeit currency or the acceptance of a false I.D. in connection with a financial transaction, will require the organization to file multiple reporting forms with law enforcement and local/state/federal agencies, such as an FBI Suspicious Activity Report (SAR) or a Secret Service Counterfeit Note Report (SSF 1604).

Fraud investigations often will require cooperation with discovery procedures conducted by law enforcement, which may involve the company's legal counsel, Sr. Loss Prevention and/or Sr. Accounting executives to become involved, thus further utilizing their valuable time to deal with what may have initially been a minor event.

Fraud soft costs may also include punitive fines and penalties assessed against organizations for failure to comply with legislative guidelines. Finally, organizations may be forced to comply with audits and additional paperwork burdens as a result of being placed on "fraud watch" or "high risk" lists by the FTC, the IRS and other government agencies.

When tallied in full, soft costs can often total 4-5 times the amount of the initial "hard cost" loss. Thus, a simple $100 counterfeit currency loss can easily balloon into a total cost to the company of $500-$600.

REGULATORY COMPLIANCE

Organizations in the United States operate under a complex regulatory structure of overlapping federal, state and local statutes. This is particularly true as it relates to conducting transactions with the public. Businesses are required to establish programs to verify the identity of individuals with whom they conduct many different types of transaction. In addition, they must maintain records of such identification verification procedures for years after the date of the transaction, in a manner that adheres to strict legislative guidelines regarding information privacy and data security.

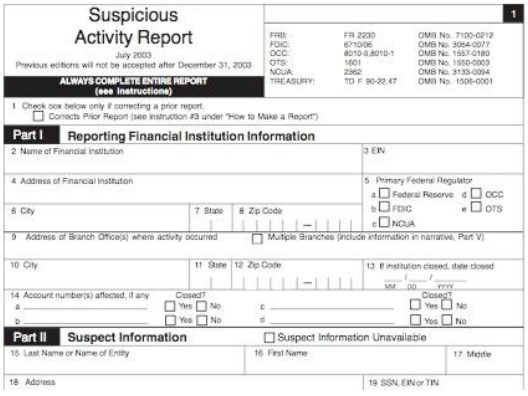
TRANSACTIONS REQUIRING COMPLIANCE MANAGEMENT

Financial Account Transactions

In 1970, congress passed the Bank Secrecy Act ("BSA") requiring Financial Institutions ("FI's") to become proactively involved in anti-money-laundering activities by monitoring and reporting on transactions that appear suspicious. Since 2001, with the passing of the USA Patriot Act, an amendment to the BSA, FI's have been tasked with preventing identity fraud and to mitigate the impact of identity fraud on individuals.

The range of businesses classified as Financial Institutions include banks and credit unions as well as other business entities such as auto dealers, mortgage brokers, utility companies and telecommunications companies. Any business that is involved with account types that are covered under an umbrella of different legislative acts are required to create compliance programs. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking and savings accounts, and in some cases business accounts where this is a foreseeable risk of identity fraud.

Filing of Suspicious Activity Report (SARs) is critical to filter unusual or suspect transactions. On December 4, 2003, President Bush signed into law the Fair and Accurate Credit Transactions Act (FACTA) to provide consumers with increased protection from identity theft. Six agencies were involved in drafting the rules: the Treasury Department's Office of Thrift Supervision, the Office of Comptroller of the Currency, the FDIC, the FTC, the National Credit Union Administration and the Federal Reserve System. The Red Flags Rule amended FACTA in 2008 and requires FIs to get more serious about protecting consumers from identity fraud.



Suspicious Activity Report

July 2003

Previous editions will not be accepted after December 31, 2003

ALWAYS COMPLETE ENTIRE REPORT (see instructions)

FRB: FR 2230 OMB No. 7100-0212
FDIC: 6710/06 OMB No. 3064-0077
OCC: 8010-9,8010-1 OMB No. 1557-0180
OTS: 1601 OMB No. 1550-0003
NCUA: 2362 OMB No. 3133-0094
TREASURY: TD F 90-22.47 OMB No. 1506-0001

1 Check box below only if correcting a prior report.
☐ Corrects Prior Report (see instruction #3 under "How to Make a Report")

Part I Reporting Financial Institution Information

2 Name of Financial Institution | 3 EIN

4 Address of Financial Institution | 5 Primary Federal Regulator: a ☐ Federal Reserve b ☐ FDIC c ☐ NCUA d ☐ OCC e ☐ OTS

6 City | 7 State | 8 Zip Code

9 Address of Branch Office(s) where activity occurred ☐ Multiple Branches (include information in narrative, Part V)

10 City | 11 State | 12 Zip Code | 13 If institution closed, date closed (MM DD YYYY)

14 Account number(s) affected, if any — Closed? a ☐ Yes ☐ No b ☐ Yes ☐ No c ☐ Yes ☐ No d ☐ Yes ☐ No

Part II Suspect Information ☐ Suspect Information Unavailable

15 Last Name or Name of Entity | 16 First Name | 17 Middle

18 Address | 19 SSN, EIN or TIN

Covered entities must create a written identity theft program designed to detect, prevent and mitigate identity theft in connection with certain covered accounts (the "Red Flags Rule"). Businesses must build transaction level, processes and organizational initiatives to avoid identity theft and related fraud losses. They are required to have Customer Identification Programs (CIP), Know Your Customer (KYC) programs and systems in place regarding terrorist financing and anti-money laundering.

BSA

Congress enacted the Bank Secrecy Act (BSA) in 1970 to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, criminal activity. The U.S. government continues to use the BSA today as a tool to fight drug trafficking, money laundering and other crimes.

The BSA requires banks to maintain financial transaction records in a manner that allows them to be reconstructed to assist with government investigation of certain crimes. It also requires banks to report certain types of transactions to government agencies within a specified time after the transaction takes place.

Congress has amended the BSA a number of times to enhance its law enforcement effectiveness. Most recently, the USA Patriot Act of 2001 added provisions to deter the use of financial institutions as financial conduits for terrorist activities and operations.

In order to comply with the BSA, banks and other financial institutions must understand a range of requirements, which involve maintaining systems and controls, training employees and knowing who customers are.

Examples of businesses that are "financial institutions" for purposes of the BSA:

- Mortgage lender or broker
- Check casher
- Pay-day lender
- Credit counseling service and other financial advisors
- Medical-services provider that establishes for a significant number of its patients long-term payment plans that involve interest charges
- Financial or investment advisory services including tax planning, tax preparation, and instruction on individual financial management
- Retailer that issues its own credit card
- Auto dealers that lease and/or finance
- Collection agency services
- Relocation service that assists individuals with financing for moving expenses and/or mortgages
- Sale of money orders, savings bonds, or traveler's checks
- Government entities that provide financial products such as student loans or mortgages

A bank's BSA program must, at a minimum, do the following:

(a) Designate an individual or individuals as responsible for coordinating and monitoring day-to-day compliance. Most banks appoint a senior—level person as a BSA officer with authority to set and enforce bank policies.

(b) Provide for a system of internal controls to ensure ongoing compliance. Internal controls should include systems to detect, report and monitor large cash transactions and suspicious activity; ensure adequacy of the customer identification program; and promote adherence to Office of Foreign Assets Control (OFAC) rules. A sound monitoring system includes independent analytical review of transactions.

(c) Provide for independent testing. A comprehensive independent review is conducted at least annually.

Customer Identification Program

All FI's must verify the identity of individuals wishing to conduct financial transactions. Section 326 of the USA Patriot Act requires FI's to develop a Customer Identification Program (CIP) appropriate to the size and type of its business. Each FI must incorporate a CIP into their Bank Secrecy Act/Anti-money laundering compliance program.

CIP requires, at a minimum, reasonable procedures for

(i) verifying the identity of any person seeking to open an account;
(ii) maintaining records of the information used to verify the person's identity; and
(iii) determining whether the person appears on any lists of known or suspected terrorists provided to the Financial Institution by any government agency.

Customer Identification Program

It will be important for your organization to identify the types of identification documents you will deem acceptable.

For maximum reliability, primary IDs should be government issued and should bear a picture of the customer. A customer could identify himself, for example, by producing one form of primary ID and one secondary ID. In order to be acceptable, the ID should be unexpired. Since some IDs (such as the recently issued military IDs) no longer bear a signature of the individual, you'll want to request another form of ID that gives you a specimen signature. By the same token, since many driver's licenses and state IDs no longer include a Social Security number, you will need to either look to a second document to verify the SSN, or you will need to use a third-party database to confirm the number given to you.

In addition, you should educate your frontline personnel about how to examine an ID, and should equip your staff with the resources necessary to determine the validity of identification documents that are issued by someone other than your state.

The FI must establish risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must specify the identifying information the FI must obtain from each customer prior to opening an account and at a minimum contain the following:

* Name
* Date of birth (for an individual)
* Identification Number:
    - o For a U.S. resident, a taxpayer ID number (SSN, ITIN)
    - o For a non-U.S. person who does not have such a number, the FI may obtain an identification number from some other form of government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

FIs are encouraged to obtain more than one type of documentary verification to ensure that it has a reasonable belief that it knows the customer's true identity. FIs are encouraged to use a variety of methods to verify the identity of a customer.

Controlled Product Sales

Businesses that sell restricted products must adhere to a separate set of regulatory guidelines. Alcohol and tobacco laws are typically set at the state or municipal level. Laws dealing with the sale of prescription drugs and over-the-counter pharmaceuticals can be mandated at the federal or state level. Regardless of the source of the legislation, businesses are driven by both an ethical imperative to adhere to the restrictions as well as a financial need to avoid punitive actions such as fines and suspension of sales licenses that may result if they fail to follow regulatory guidelines.

Alcohol & Tobacco

- Alcohol

Underage drinking is a major public health problem in the United States. Over 12 million underage youth drink annually. In 2005, they consumed 15% of all alcohol sold in the United States, totaling $19.8 billion in sales, and providing profits of $3.6 billion to the alcohol industry. All States prohibit furnishing alcoholic beverages to minors. The National Minimum Drinking Age Act of 1984, also called the Federal Uniform Drinking Age Act, was passed on July 17, 1984 by the United States Congress. The act requires all states to legislate and enforce the age of 21 years as a minimum age for purchasing and publicly possessing alcoholic beverages. State law may permit local jurisdictions to impose requirements in addition to those mandated by State law.

Example Penalties Faced by Liquor Retailers

*Minors in a public premises (bar/green license): penalty for licensee is maximum penalty of $1000 and/or 6 months in county jail

*Minors in a public premises (bar): penalty for minor is fine not less than $200

* Sale during prohibited hours: maximum penalty of $1000 and/or 6 months in county jail

* Sale to minors: maximum penalty of $250 and/or 24-32 hours Community Service

* Sale to minors - 2nd offense: maximum penalty of $500 and/or 36-48 hours of Community Service

* Furnishing alcohol to a minor: $1000 and 24 hours Community Service

* Furnishing alcohol to a minor resulting in great bodily injury or death: minimum 6 months in jail and/or maximum $1000 fine

(State of California Alcoholic Beverage Commission)

Retailers are responsible for insuring that sales of alcoholic beverages are made only to persons who are legally permitted to purchase alcohol. Inspecting government-issued identification (driver's license, non-driver identification card, passport, military identification) is one major mechanism for insuring that buyers meet minimum age requirements. In attempting to circumvent these safeguards, minors may obtain and use apparently valid identification that falsely states their age as 21 or over. Age may be falsified by altering the birthdate on a valid identification, obtaining an invalid identification card that appears to be valid, or using someone else's identification.

Compliance check studies suggest that underage drinkers may have little need to use false identification because retailers often make sales without any inspection of identification. However, concerns about false identification remain high among educators, law enforcement officials, retailers, and government officials. Current technology, including

high quality color copiers and printers, has made false identification easier to fabricate, and the Internet provides ready access to a large number of false identification vendors.

- Tobacco

The ease with which adolescents can purchase tobacco products underscores the reasoning behind a system of civil penalties to retail owners for illegal sales, including suspension or revocation of a tobacco sales license for repeat offenders. Currently, all states have laws to penalize the business owner, manager and/or clerk for first violation of selling tobacco to minors. Twenty-three state laws include the possibility of suspension or revocation of a license to sell tobacco products for violation of youth access laws. Research indicates that strong enforcement of minors' access laws might reduce tobacco use among youths. Therefore, consistent and aggressive enforcement of minor access laws have been enacted in an effort to alter retailer behavior.

Every person, firm, or corporation that knowingly sells, gives, or in any way furnishes tobacco products or paraphernalia, including blunt wraps to a minor is guilty of an infraction and shall be subject either to criminal action or??. The penalty or penalties to the business for selling cigarettes to minors varies by state. The penalties for selling cigarettes to a minor range from a written warning, to minimum monetary penalties that range up to $500, and maximum monetary penalties that ranged from $25 to $2,500. In California, the penalty for three offenses (which include either sales of tobacco or paraphernalia to youth) is $1000, while in Alaska, a retailer's license can be suspended for up to 90 days after three offenses. In Texas, after four offenses in one 12-month period, a retail license may be revoked

Affirmative Defense
If a defendant, or their employee or agent, demanded, was shown and reasonably relied upon a facsimile of or a reasonable likeness of a document issued by a federal, state, county, or municipal government, or subdivision or agency thereof shall have a defense against prosecution.
CA PENAL CODE § 308 (2006)

Pharmaceuticals and Over-The-Counter Drugs

Operating a pharmacy means adhering to a wide set of federal and state regulations governing everything from customer privacy to the physical layout of your facility. Pharmacies have to stay up to date on these regulations or they could face steep penalties.

The Federal Food, Drug, and Cosmetic Act (FD&C Act) requires that before many restricted drugs can be dispensed, pharmacists must obtain proof of identity from cash purchasers or individuals buying threshold quantities. Proof of identity must be in the form of a driver's license, one additional form of identification and the purchaser's signature.

The federal regulation, Combat Methamphetamine Epidemic Act of 2005, requires retailers to track the sale of all products containing pseudoephedrine, ephedrine, and phenylpropanolamine and includes non-liquid forms, liquids, gel caps and pediatrics. It is

up to the drug retailer to develop and implement a pseudoephedrine sales policy that complies with all federal regulations. At a minimum, the seller must maintain a written or electronic list (logbook) of sales that identifies:

(1) Products by name;
(2) Quantity sold;
(3) Names and addresses of purchasers; and,
(4) Date and time of the sales.

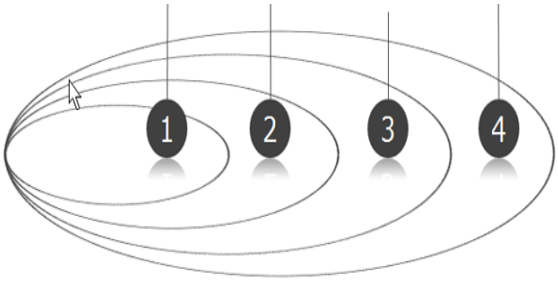
The retailer may not sell the product unless prospective purchaser presents a photographic identification card issued by a State or the Federal Government. Purchaser must sign the logbook and enter his or her name, address, and date and time of sale. The retailer must determine that the name entered into the logbook corresponds to the name provided on such identification and that the date and time entered are correct. The retailer must enter into the logbook the name of the product and the quantity sold.

Failing to meet the federal regulations regarding pharmaceutical sales could result in serious civil and criminal penalties. Violations of any of these provisions are subject to a civil penalty of up to $25,000. If a violation was knowingly committed, the penalty is increased to imprisonment of up to one year, a fine of up to $25,000, or both. Repeat offenses can be subject to a prison term of up to two years, a $50,000 fine, or both See 21 U.S.C. 842(c).

LAYERED SOLUTIONS

Addressing the multiple points of potential vulnerability to fraud loss and ID-verification related regulatory compliance violations requires a systemic approach to risk analysis. Modern business organizations may involve diverse activities, including physical store operations, finance departments, "covered" financial transactions, sales of controlled products and acceptance of a broad range of payment types. Such activities must be evaluated with an eye towards scope, type and depth of risk at each point where the organization conducts a public-facing transaction.

Fraud Fighter™ believes a sensible approach to solving these mixed exposures to varied counterfeit transaction fraud and distinct opportunities for failed compliance with regulatory requirements is to construct an intelligently "layered" approach to the problem. Such an approach matches the features and functionality of the solution to the preventative and compliance need at each individual point of transaction.



However, no solution can be meaningful if it cannot be purchased at a cost-effective price which provides a rapid and considerable return-on-investment. This is where the concept of "multi-layered" really achieves, because the goal of the solution is to place "tiered" security layers, with low cost solutions employed in those areas with lesser exposure, and employing "high-end" equipment only where the needs assessment determines it is imperative to have it to mitigate against high levels of risk, comply with legal frameworks, control losses from fraud, or otherwise.

MULTIPLE POINTS OF VULNERABILITY

No two organizations are alike. Even companies that are often compared to each other as "peers" will have unique requirements and varied exposure to different vulnerabilities. Similarly, no two points of transaction are the same. For this reason, it is not advisable to try to force an out-of-the-box solution to meet the needs of a company without first understanding what the problems and potential vulnerabilities are.

As an example, we could discuss the diverse operations of a large "grocery store" chain with whom Fraud Fighter has consulted and provided our solutions to. Our initial understanding of the transaction environment was that this type of operation performed a high-volume of relatively low-value transactions with a transient customer base. On average, the stores operated 13 cash-wrap locations. Accordingly, the initial discussions driven by the customer were focused on the need to validate payment forms and to verify ID's for alcohol and tobacco product sales.

However, after learning in detail about the operations, we discovered that some of the greatest operational problems they had were associated with the "covered" financial transactions they conducted. Sales of money orders and electronic funds transfers to both

domestic and international locations triggered a slew of regulatory compliance issues and reporting requirements. One Southern California region, alone, had seen greater than 25 separate IRS audits in one quarter in connection with the sale of money orders and wire transfer services.

In addition, the sale of PPA compounds (AKA, ephedrine, a pre-cursor chemical required for methamphetamine production) and the operation of a pharmacy also created the need to log and record identities of some customers.

In response, Fraud Fighter proposed a "multi layered" approach to address these vulnerabilities. At the cash-wrap locations, basic counterfeit detection devices (i.e. UV devices) were installed. At the customer service counter where money orders and wire transfers are processed, UV devices are installed alongside Image Capture devices to capture and securely store images of ID documents presented in order to comply with Red Flag, Customer Identification Program and Know Your Customer requirements. The same Image Capture device at the customer service counter is used to log ID's for purchase of ephedrine products. The Customer service desk also uses an electronic currency verifier to quickly scan high-denomination banknotes presented at the time money orders and wire transfers are conducted. At the pharmacy, a separate Image Capture unit is installed to log medical cards and ID documents for all purchases of Class I narcotics. Finally, in the back-office, the FF-1000 is used to quickly perform a double-check on cash-drawer reconciliation counts.

The "Displacement Effect"

This is a phrase Fraud Fighter coined after hearing the same observation from numerous customers. We have frequently found companies willing to address their "problem fraud stores" by placing our equipment into the stores where they are experiencing the highest levels of fraud. Afterwards, the LP staff would relate that problems in the stores with Fraud Fighter equipment had virtually disappeared, but the stores that previously had no problems were now showing signs that the criminals had focused their attentions on them because they didn't have Fraud Fighters. For LP managers who were given bonuses based on improved fraud numbers, those who had our equipment were at a distinct advantage over their peers!

This "Displacement Effect" underscores an important fact about fraud prevention. Criminals will exploit any weakness they can find. Layered solutions help to plug the vulnerabilities.

TRANSACTION FRAUD SOLUTIONS

To be effective, a fraud-prevention tool must actually be used by the transaction-level employee. To ensure that this happens, the solution must be conveniently located and simple to use during the transaction process – not slowing down the pace and not offending the customer.

For this reason, Fraud Fighter has, since the date the business first started, designed and sold a line of simple fraud detection equipment. Fraud Fighter Ultra-Violet equipment provides a number of unique value propositions for transaction fraud prevention, while our more advanced electronic bill scanners and age verification machines provide high-confidence detection and stand-alone functionality.

Fraud Fighter equipment are very **LOW COST** tools. Even complex store operations requiring multiple units to secure dozens of cash-wrap locations can see their monthly costs to equip the stores total less than $50.

Fraud Fighter equipment has a **HIGH IMPACT** on the business. The ability to detect counterfeit currency, credit cards, negotiable instruments and ID's *while the transaction is occurring* has proven time and time again to reduce losses, increase compliance and minimize follow-up case management work required to investigate fraud events.

Fraud Fighter equipment offers **MINIMAL DISRUPTION** to store operations. Because the primary fraud-prevention tools are stand-alone, there is no need for integration with existing systems, or connecting to a network. "Plug and play" is one of the key benefits. Also, the tools are simple and intuitive to use, requiring very little training.

Fraud Fighter equipment offers **HIGH ROI**. Break-even is often seen by customers within several weeks of purchase, and some of our larger customers have experienced ROI multiples of 40-1 or greater in the first year.

TRANSACTIONAL COMPLIANCE SOLUTIONS

At the heart of most regulatory compliance issues lies the ability to validate identification authenticity. Whether observing the requirements of "covered financial transaction" legislation, age restricted product regulations, or the sale of controlled pharmaceuticals/prescription compounds, the central principal guiding organizations is to ensure that they certify who the person is by conducting a validation of the ID document.

Much regulation was passed through state and federal legislatures without addressing the specifics of HOW such ID authentication is to be performed. For example, Section 326 of the USA Patriot Act requires FI's to develop a Customer Identification Program (CIP) "appropriate to the size and type of its business." The burden was placed on businesses to determine how to comply. In most cases, no thought was given as to whether a viable commercial solution existed to resolve the needs created by the new laws.

Fraud Fighter believes that the solution to this challenge is to conduct a needs-analysis of the organizational operations. Reviewing the type, transaction volume and profile of each "public facing" point of transaction enables the organization to then match appropriate tools to each location. Some locations may only require "validation of ID", while other locations may demand "authentication" together with "logging and secure storage" of the ID information.

A "layered approach" to resolving compliance is achieved by enabling every step in the transaction process – each a potential point of vulnerability – to be shielded with a product that is appropriate both functionally and financially to its place in the security chain.

CONCLUSIONS

Organizations lose revenues from the effects of counterfeit fraud and from non-compliance with transactional regulations. Such losses are significant enough to deserve the attention of management. Increasingly complex regulatory regimes and a constantly changing counterfeit landscape create new, unique exposures to losses on a daily basis. Businesses can no longer choose to ignore these issues.

Counterfeit fraud is a multi-hundred-billion dollar per-year problem. It is, therefore, reasonable to assume that any business which conducts transactions with the public will, at some point, experience losses from fraudulent payments – whether through fake money, fraudulent credit cards or other counterfeit instruments. It is equally reasonable to assume that when the total loss from a fraudulent event is tallied, considering both the hard and the soft components, the cost of any single fraud event is likely to exceed the cost of the tools necessary to prevent such events from happening.

Regulatory compliance requirements are on the rise. The breadth and variety of transactions which now require some form of identification validation is surprisingly large. The regulatory environment is only likely to become progressively more complex as additional industries come under the scrutiny of government departments charged with security, anti-terrorism and public health. In many cases, the negative consequences of failure to comply with a regulatory requirement may be sufficient to either cause bankruptcy or turn a profitable store into a money losing location.

A logical approach to addressing these problems is to conduct an evaluation of the organization's operations with an eye towards identifying the nature and scope of exposure to potential losses. Many organizations operate diverse businesses with widely variable transactional activity throughout their different business processes. Thus, it is sensible to evaluate each point of transaction and to target fraud prevention and compliance management equipment appropriate to each location. This "layered" approach produces a solution that matches needs with requirements in the most cost-effective manner possible.

Rather than force a "one size fits all" solution onto real world conditions, customizing a catalogue of available solutions to each point of transaction can secure an organization against its exposure.