CONTACT:
Research Section
5000 NASA Blvd., Suite 2400
Fairmont, WV 26554
Ph: 304-367-1994
Fax: 304-366-9095
Web: www.nw3c.org

Check Fraud (August 2015)

Check Fraud is the forgery, alteration, counterfeiting, or knowing issuance of a check on an account that has been closed or has insufficient funds to cover the amount for which the check was written.[1] The preceding is a quote from a 1999 report published by the Office of the Comptroller of the Currency, a division of the U.S. Treasury. In less than 20 years since that report was published, the problem the report attempts to address has changed considerably. The changes are due primarily to advances in technology that have significantly altered the landscape in money handling and finance. Use of the written check has declined noticeably in the just the past ten years. One source sites a 28% reduction in the use of written checks in just the short period between 2006 and 2010.[2] According to a recent report from the Federal Reserve's Cash Products Office, in 2000, checks were used in more than 40 billion transactions; as of 2012, that number is down to less than 20 billion.[3] Yet, as a society, we still depend on checks to a significant degree and the problems surrounding the fraudulent use of the instrument are continuing to challenge the criminal justice system.

- 71% of organizations are victims of some kind of fraud each year, 93% of those fraud attempts involve a check.
- Checks are the most popular form of payment for business-to-business transactions, estimates are around 80%.
- Only 2% of criminals that commit check fraud end up in jail.[4]

In this report, we will attempt to justify the current state of affairs in finance; however, we feel a bit of historical background will be useful in understanding how things have evolved to where we are today. The comparison and the speed which these changes took place should provide some insight into a portion of the problem faced by the banking industry in just keeping pace with the technological changes and attempting to balance the convenience of their customers against the challenges presented by security issues.

How It Happens

Although, as we already noted, the use of paper checks is quickly disappearing from use due to rapidly developing advances in electronic funds transfers, debit cards, and new concepts for paperless and cashless value transfer systems using a growing list of mobile devices including cell phones, tablets and smart watches, there are still those who prefer to write checks and business applications where the written check is the preferred method of funds transfer.

For the sake of historical background, check processing used to be not only time consuming but costly. At one time, checks were required to be presented to the banks where they were drawn on for inspection and signature verification purposes before being honored even though, typically, signature verification was only done for high-value checks or when there was reason to be suspicious of the account. This requirement of physical presentment naturally resulted in considerable air and land transportation costs. It also resulted in delays of anywhere from one to ten business days, or what came to be called "float" time.

> "…from 1 to 5 days, averaging 1 day for local or within-city checks and usually 2 to 3 days for non-local items such as checks going from one city to another across the country."[5]

The above does not account for weekends and presumes that there are no bank holidays that will necessarily extend the float time.

This all changed with the terrorist attacks of 9/11 when the physical transportation of checks across country became impossible for several days because all air traffic was suspended. The float time was extended to more than eight times the normal period and as a result, the cost of using checks due to delays in the process of transportation and collection rose to $47 billion.[6] A direct result of this was the passage in 2003 of legislation entitled "The Check Clearing for the 21st Century Act" which became known by its shortened name, *Check 21*.

> "The Check Clearing for the 21st Century Act (or Check 21 Act) is a United States federal law (public Law 108-100) enacted into law October 28, 2003 by the 108th Congress. It took effect one year later, on October 28, 2004. The law allows the recipient of a paper check to create a digital version, thereby eliminating the need for further handling of the physical document. It paves the way for the industry to save billions of dollars and increase the speed in which checks are processed."[7]

This legislation allowed the use of digital technology that had existed for some time involving digital imaging and transmission of documents to be used to eliminate or significantly reduce the costs and time delays involved in processing of checks. It also reduced the dependence on physical transportation of the check itself which in turn, reduced the impact on the financial system of another event like 9/11 where air traffic is suspended or reduced.

Check 21 currently permits almost all of the 24.5 billion checks paid annually in the U.S. (worth $32 trillion) to be processed electronically on a same-day (or next-day) basis once they are deposited at a bank.[8] For recordkeeping purposes, when the digital image of a check is transmitted to its intended location, a substitute check is generated which is allowed to legally represent the original document. Regardless of how much more efficient *Check 21* seems to have made the transmission of funds, however, the system is still vulnerable to fraud.

In the past, a variety of techniques have been used to commit check fraud, including writing checks on closed accounts, purposely writing a check on an account with insufficient funds to cover it, opening fictitious accounts, alteration of an original check, forgery, and counterfeiting. These techniques have changed somewhat with the availability of technology and banking policies aimed at making funds transfers easier for their customers. In some ways these changes have made it better for the customer in terms of security and convenience; however, in some ways these changes may make it easier to commit fraud.

Traditional Forms of Check Fraud: [9]

- **FORGED SIGNATURES**--legitimate blank checks with an imitation of the payer signature;
- **FORGED ENDORSEMENTS**--often involves the use of a stolen check, which is then endorsed and cashed or deposited by someone other than the payee;
- **COUNTERFEIT CHECKS**--due to the advancement in color copying and desktop publishing capabilities, this is the fastest-growing source of fraudulent checks today;
- **ALTERED CHECKS**--information on a legitimate check, such as payee or check amount, changed to benefit the perpetrator; and
- **CHECK KITING**--the process of depositing a check from one bank account into a second bank account without the funds available in the account the check is written on.
- **CHECK WASHING:** the process of altering a check using a chemical to remove original information such as who the check is made out to or the amount, and altering it to indicate another recipient or a higher amount.

Prior to digital technology, forgery was almost an art form that required significant skill to perform. Today, one needs no special artistic abilities, just a simple scan of a legitimate copy of a person's signature will allow the manipulation (removal from one document and placement on another) of that signature using relatively inexpensive, easily available computer software designed to make such modifications almost invisible to the naked eye and a laser printer of reasonable quality, all of which are available at the local office supply store. This would allow the perpetrator to affix a scanned signature to a check which can then be deposited into an account electronically. The deposit normally appears in the recipient's balance within minutes and the funds can then be used, at least until such time as the fraud is discovered by the bank or the original owner of the account. Depending on how attentive the owner of the account is to daily transactions, the crime could go unnoticed for some time. Investigation and prosecution are often complicated due to the skills needed to forensically determine first that the document was altered and second, just who was responsible for the manipulation. The internet has made it possible to make such transactions from almost anywhere in the world, and to disguise the point of origin to the point of being almost impossible to determine where the original illegal act originated from.

The actual creation of counterfeit checks is also made significantly easier by today's technology and the ability to scan and deposit checks remotely using a cell phone or presented at a bank for cash. All it takes is access to a legitimate check from any financial institution, a scanner and the appropriate software, and a quality laser printer to create a blank check capable of being passed off as coming from the original owner of the account. Until recently, the use of the unique characters that appear at the bottom of a check along with the ink they are printed with was one of the security measures used by banks to combat check fraud. The MICR (magnetic ink character recognition) codes at the bottom of a check are what was being read by the scanning machines located at most checkouts and bank teller locations when a check was presented for cashing or deposit.

> The characters are printed with special MICR Fonts and are known as MICR Characters, which must be printed with MICR Toner or MICR Ink. It is the combination of Toner and Fonts that create the machine readable MICR line.[10]

Recent practices by most major banks allowing the use of cell phones to photograph checks for deposit have negated the use of the MICR, at least to some degree, as a security method. Such transactions simply require the use of the high-definition cameras now standard on cell phones to photograph both the front and back sides of a check which is then deposited in the users' account. The cameras do not have the ability to ascertain whether the MICR inscriptions are produced using the magnetic ink or are simply a high-quality reproduction of the image of a MICR code. Producing convincing looking documents is a comparatively simple task with the right tools. All a perpetrator needs is a sample of what a legitimate check looks like to defraud the owner's account. Certainly, these actions should be traceable by an investigator with access to with the skills to perform the required computer forensics, but with enough skill, the electronic trail left by someone committing a crime via the internet can easily be disguised so as to make investigation and prosecution difficult, if not impossible, in some cases. Meanwhile, it would likely make funds available to a fraudster, at least for an even short period of time, which could certainly be enough time to make off with money from the owner's account.

Following is a discussion of the various ways in which check fraud would be perpetrated dealing specifically with paper checks. Assuming access to the proper tools discussed above, it takes little imagination to figure how the following forms of check fraud could be performed in today's world with the right kind of technology available.

Closed account fraud, or "paperhanging," occurred when checks were written against an account that has already been closed. This type of check fraud relied upon the float time that existed prior to *Check 21* legislation. The float time offered a window of opportunity for the criminal to defraud the financial institution. A suspect would typically attempt to cash a check at a local branch of the bank or at a place of business within a short time after closing the account on which the check is drawn.[11] The almost instantaneous ability to perform transactions presented by today's technology may have made this form of fraud a bit more difficult. Calling the bank to notify them that you want your account closed usually prompts action by the teller to close the account and make funds inaccessible, while you are on the line, making it almost impossible to conduct this form of check fraud.

Check Kiting: An act similar to closed account fraud is known as check kiting. Check kiting requires multiple bank accounts and the movement of fictitious funds between those multiple bank accounts. An explanation of how check kiting works is presented by the Legal Information Institute at Cornell Law School.

> "A crime involving writing a check on an account, Account A, with insufficient funds and depositing it in another account, Account B, and then writing a check on Account B and depositing it in Account A to cover the first check written on Account A. Kiting takes advantage of the time it takes banks to clear checks. Before the bank in which Account B is held has time to clear the check written on Account A, the kiter has already written a second check on Account B and deposited it in Account A, making it appear as though the bank in which Account A is held has sufficient funds. The bank in which Account B is held then honors the check written on Account A. Through kiting, the kiter obtains an illegal, interest-free loan."[12]

Like closed-account fraud, the check kiter also takes advantage of the time that it takes for a bank transaction to be processed in order to create fraudulent balances. Technology has made a lot of what used to be common in check fraud, no longer possible. According to Experian, a credit

tracking and reporting agency, things have changed considerably in the last few years due to advances in technology and the ability to almost instantaneously check an account.

> "In the past, the float period could be several days because it took that long for the business to mail the check to the bank and the bank to then manually process it. Today, many, if not most, transactions are electronic. Now, the check often is scanned at the point of sale and the information is immediately transferred to the bank for processing. Float is almost eliminated."[13]

Check fraud can be facilitated through the use of false information to open new accounts, such as in cases of identity theft. After depositing altered or counterfeit checks into the account, the offender then makes withdrawals for a large portion of the account balance before the bank realizes it has been victimized.[14] At this point, the perpetrator can then use one bad check from the falsified account to open another account at a different bank and engage in the check kiting process, working the system until the bank catches up to the scheme.

Reductions in float time would not necessarily affect the frequency with which this type of activity takes place as the bank would have little reason to suspect inappropriate activity until the person whose identity had been stolen realized they had been victimized and reported it to the authorities. Depending on the circumstances of the individual incident, this could afford the perpetrator sufficient time to do considerable damage.

Check Washing: The process of altering a check is another form of check fraud. Chemical modification to checks or "check washing" is one of the most popular forms of alteration.[15] Check washers used acid-based household chemical solutions to alter or erase particular pieces of information on the checks such as payee name and payment amount. Check washers would then add new information to the checks using a typewriter, laser printer, or other means in order to make the checks payable to themselves or to co-conspirators while also increasing the amount payable.[16]

Again, digital technology has had an impact on this activity with high-quality digital printers and computer software making it unnecessary to "wash" a paper document with some chemical to eliminate the original markings on the check. Using a scanner, a home computer and a laser printer all available at any office supply store, someone with limited technical skills can perform essentially the same process as the check washer, by scanning a check, making the needed alterations, printing an altered copy of the original document and then scan and transmit it to a bank account for deposit. Once deposited, the funds are available for use until such time as the bank is able to determine that the account the check was drawn on was actually false.

There can be little doubt that technology has played a major role in the proliferation of check fraud. The use of relatively inexpensive computers, scanners, and printers has enhanced the ability of criminals to manufacture their own brand of counterfeit checks. Counterfeiters, with the aid of computers, can duplicate corporate and payroll checks, travelers' checks, credit cards, certified bank checks, money orders, currency, and other negotiable instruments, as well as personal identification such as driver's licenses and social security cards. "Some fake checks look so real that bank tellers are reporting being fooled."[17]

Regardless of the changes that have taken place over the past decade, the evolution of the way in which we do business, from paper documents (checks) to digital transfers, does not seem to have reduced the problem of check fraud. According to the 2014 AFP Payments Fraud and Control

Survey, "Checks continue to be the dominant payment form targeted by fraudsters, with 82 percent of survey respondents indicating that checks were targeted at their companies."[18]

Costs and Statistics

- According to the 2014 AFP Payments Fraud and Control Survey, "In most instances, actual or attempted payments fraud has resulted in relatively small financial losses. For 39 percent of organizations, the potential loss from fraud is estimated at less than $25,000; for 37 percent of organizations the potential loss is between $25,000 and $249,999. The potential loss is $250,000 or more for 17 percent of organizations."[19]

- According to a survey by the American Bankers Association, "Fraud against bank deposit accounts cost the industry $1.744 billion in losses in 2012, according to ABA estimates. Debit card fraud accounted for more than half of 2012 losses (54 percent), followed by check fraud (37 percent).[20]

- According to the *2013 Federal Reserve Payments Study*: Checks (consumer and business) were the payment instrument with the highest average value of unauthorized transactions in 2012. The average unauthorized check transaction was valued at $1,221 as compared to ACH at $730, ATM withdrawals at $217, general purpose credit cards at $138, and general purpose debit cards at $105.[21]

- In FinCEN's most recent *SAR Activity Review, By the Numbers*, published in June 2010 and covering all of calendar year 2009, it was noted that 27% of the suspicious activity reported by depository institutions in 2009 can be attributed to fraud-related activities, and that check fraud was one of only two categories that has seen an ***increase*** in SARs every year between 1996 and 2009.[22]

Examples/Case Studies

- John Dale Henegar, 42, admitted that on February 17, 2005, he presented to Home Federal Bank for deposit and withdrawal, a check in the amount of $1,843,322.39 that was payable to "JOHNSGIFTS (CHEQUE # 222361) 101 APRIL LANE LAFOLLETTE, TENNESSEE 37766 REF: JOHN HENEGAR" and drawn on a Bank of Montreal account of Agilysys Canada, Inc. (hereinafter "the $1.8 million Agilysys check"). For the purpose of inducing Home Federal Bank to accept and deposit the $1.8 million Agilysys check, Henegar falsely represented to Home Federal Bank that he had received the $1.8 million Agilysys check as payment for a "computer software program" that he had sold to Agilysys Canada, Inc. for $1,843,322.39. On February 24, 2005, relying on Henegar's fraudulent and material misrepresentation and inter-bank automated clearinghouse verification procedures, Home Federal Bank made the proceeds of the $1.8 million Agilysys check available to Henegar. The $1.8 million Agilysys check had originally been payable to International Business Machines. Prior to being indicted, Henegar had admitted to law enforcement agents that "in terms of the Agilysys check I knew this check was a scam." [23]

- Terry Massengill, 36, of Bellflower, California, perpetrated the fraud by paying Wells Fargo employees to access and steal customer bank account information and provide it to

Massengill. Throughout the fraud, Massengill and co-conspirators arranged to have checks in the names of legitimate Wells Fargo customers delivered to various addresses in multiple states. Checks were then forged and cashed in amounts that ranged from several thousand dollars to, in one case, $42,000. Co-conspirators who acted as check-cashers or "runners" would then return a portion of the funds to defendant Massengill. In addition, Massengill arranged for a co-conspirator to impersonate account holders and answer phone calls from Wells Fargo Bank employees seeking payment authorization. Massengill did this by altering the phone numbers associated with the account, then routing the calls to a phone number under his control. Wells Fargo has since modified its fraud prevention security procedures so that this particular fraud tactic can no longer be used.[24]

- On September 3, 2004 Adam Weitsman was sentenced to one year and one day in prison, and agreed to asset forfeiture of $1 million. Weitsman, the operator of a recycling business in Binghamton, New York, wrote in excess of $1 billion in worthless checks over a 15-month period to perpetuate a check kite. These checks were deposited by Weitsman at Partners Bank & Trust, Binghamton, New York, and Community Bank, Olean, New York, as a means of obtaining cash to meet the operational needs of his business.[25]

Prevention Tips:

In a 2008 interview with U.S. News and World Reports, Money section, the inspiration for the 2002 movie "Catch Me If You Can" Frank Abagnale, convicted confidence man provided five valuable pieces of advice to avoid becoming a victim of check fraud schemes. Abagnale served five years in federal prison and only obtained early release when he agreed to assist the FBI find ways to combat the types of crimes that made him infamous. He provided five pieces of advice to help avoid falling victim to check fraud: [26]

- **Write Checks Sparingly**: when you write a check you leave a tremendous amount of information in the hands to the stranger to whom you presented it. Typically they will write even more information on the check such as drivers' license number or social security number for verification purposes. The person to whom you presented this information now has enough personally identifiable information to steal your identity.

- **Be vigilant during tax time**: Most people, who have to write checks to the IRS for taxes owed, endorse them in just that manner, with the three letters IRS on the "pay to" line. A thief stealing that envelope addressed to the IRS will find an easily alterable check that can be washed, the perpetrators name placed in the "pay to" section and then cashed. The victim won't necessarily know they have been victimized till the IRS notifies them they still owe taxes, probably several months later.

- **Use only secured mailboxes**, not the one on the front of your house. Secured mail boxes can only be opened by postal workers and as such are less susceptible to having checks stolen.

- **Treat your check books like cash**: You wouldn't leave cash laying in the console of your car, in plain view on your desk at work or even on the counter in your home. Don't leave the check book lying around either. It represents cash almost the same as legal currency.

- **Balance your checkbook** every month at least, more often is preferable. This is the best way to be aware of how much you have, but also helps in identifying when funds go missing that cant' be accounted for.

The Response/Current Efforts

"The FBI works closely with various law enforcement and regulatory entities to combat FIF. We collaborate with our partners at IRS-Criminal Investigative Division, Department of Homeland Security-Homeland Security Investigation (DHS-HSI), Financial Crimes Enforcement Network (FinCEN), and numerous other federal, state, and local law enforcement and regulatory agencies."[27]

"The U.S. Secret Service primary investigative mission is to safeguard the payment and financial systems of the United States. This has been historically accomplished through the enforcement of the counterfeiting statutes to preserve the integrity of United States currency, coin and financial obligations. Since 1984, the Secret Service's investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers, and money laundering as it relates to our core violations."[28]

"FinCEN dedicates its finite analytical resources to support those criminal investigations demanding advanced expertise in interpreting the ways money moves, involving large amounts of data, or novel situations where the insights from the specific investigation can be extrapolated and shared across the many agencies FinCEN supports. In this past year's survey of law enforcement, FinCEN's customers reported a 6 percentage point increase to 86 percent of them confirming that FinCEN's analytic reports contributed to the detection and deterrence of financial crime, for example by generating a new lead, providing information previously unknown, or resulting in the opening of a new investigation."[29]

"For More Information" Links

- U.S. Treasury Department, Office of the Inspector General, fraud alerts page — http://www.treasury.gov/about/organizational-structure/ig/Pages/fraud-alerts_index2.aspx

- Fraud Aid, a non-profit Fraud Victim Advocacy organization located at http://www.fraudaid.com/solution_center/jurisdictions/usfed-fbi.htm

- FinCEN, U.S. Treasury Department, located at

- U.S. Secret Service Investigations division *http://www.ustreas.gov/usss/index.shtml*

Maintenance and revisions: NW3C Research Department

This project was supported by Grant No. 2012-MU-BX-4004 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Endnotes

[1] Office of the Comptroller of the Currency. (1999) *Check Fraud: A guide to avoiding losses*. Retrieved from http://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-check-fraud.pdf
[2] From Check Guarantee web site located at http://www.checkguarantee.com/check-fraud.php
[3] Phillips, M. The Atlantic magazine, The Spectacular Decline of Checks, June 6, 2014 located at http://www.theatlantic.com/business/archive/2014/06/the-rise-and-fall-of-checks/372217/
[4] Ibid.
[5] Humphrey, David B. and Robert Hunt, Research Department, Federal Reserve Bank of Philadelphia, *Getting Rid of Paper: Savings from Check 21,* March 2012 located at; http://www.philadelphiafed.org/research-and-data/publications/working-papers/2012/wp12-12.pdf
[6] Ibid.
[7] What is Check 21? Located at http://www.check21.com/What-Is-Check-21.html
[8] Humphrey, David B. and Robert Hunt, Research Department, Federal Reserve Bank of Philadelphia, *Getting Rid of Paper: Savings from Check 21*March 2012 located at; http://www.philadelphiafed.org/research-and-data/publications/working-papers/2012/wp12-12.pdf
[9] National Check Fraud Center, Forms of Check Fraud, located at; http://www.ckfraud.org/
[10] Phillips, M. The Spectacular Decline of Checks. The Atlantic magazine, June 5, 2014, located at http://www.theatlantic.com/business/archive/2014/06/the-rise-and-fall-of-checks/372217/
[11] From Experian web site located at https://www.experian.com/ask-experian/20071017-the-consequences-of-writing-a-check-when-there-is-no-account.html
[12] Legal Information Institute, located at https://www.law.cornell.edu/wex/kiting
[13] Experian, Credit Advice, Consequences of Writing a Check When There Is No Account, located at; https://www.experian.com/ask-experian/20071017-the-consequences-of-writing-a-check-when-there-is-no-account.html
[14] Office of the Comptroller of the Currency. (1999) *Check Fraud: A guide to avoiding losses*. Retrieved from http://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-check-fraud.pdf
[15] Slotter, K. (1996) *Check Fraud: A Sophisticated Criminal Enterprise.* Located at; http://www.intelnet.org/documents/700/040/748/txt
[16] From Experian web site located at. http://www.protectmyid.com/identity-theft-protection-resources/types-of-fraud/check-washing.aspx
[17] Federal Trade Commission, consumer Information, Fake Checks, located at https://www.consumer.ftc.gov/articles/0159-fake-checks
[18] *2014 AFP Payments Fraud and Control Survey* p.6, by J.P. Morgan Corp. located at https://www.jpmorgan.com/cm/BlobServer/2014_AFP_Payments_Fraud_Survey.pdf?blobkey=id&blobwhere=1320639355606&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs
[19] Ibid p.7
[20] American Bankers' Assocation.. *2013 Deposit account fraud survey report.* Located at http://www.aba.com/products/surveys/pages/2013DepositAccount.aspx
[21] 2013 Federal Reserve Payments Study, located at https://www.frbservices.org/files/communications/pdf/general/2013_fed_res_paymt_study_detailed_rpt.pdf
[22] Prepared Remarks by James H. Freis, Director, Financial Crimes Enforcement Network, U.S. Department of the Treasury, Oct. 18, 2010, located at; http://www.fincen.gov/news_room/speech/pdf/20101018.pdf
[23] Federal Bureau of Investigation, *LaFollette Man Sentenced to 24 Months for $1.8 Million Check Fraud Scheme* August 11, 2010, located at http://www.fbi.gov/knoxville/press-releases/2010/kx081110.htm
[24] Culver City Patch, *Culver City Man Sentenced to 63 Months in Federal Prison for Check Fraud Scheme*, located at http://patch.com/california/culvercity/culver-city-man-sentenced-to-63-months-in-federal-pri9d1ee33216
[25] U.S. Department of Justice, *Federal Bureau of Investigation. Financial Institution Fraud Report*, fiscal Year 2004 p. 36
[26] Mullins L. "*5 Ways to Avoid Being a Check Fraud Victim*" inU.S. News & World Report, May 18, 2008 located at; http://money.usnews.com/money/personal-finance/articles/2008/05/19/frank-abagnales-tips-on-avoiding-check-fraud
[27] Federal Bureau of Investigation web site, Financial Crimes section, Financial Institution Fraud Unit. (2010). . Located at; http://www.fbi.gov/about-us/investigate/white_collar/financial-institution-fraud

[28] Scam Victim solution Center, located at http://www.fraudaid.com/solution_center/jurisdictions/usfed-secretservice.htm

[29] Message from the Director, Financial Crimes Enforcement Network, in FinCEN Annual Report, 2011, located at; http://www.fincen.gov/news_room/rp/files/annual_report_fy2011.pdf