

The SAR Activity Review *Trends Tips & Issues*

Issue 19

In focus: Foreign Corruption

Published under the auspices of the BSA Advisory Group.
May 2011



The
SAR
Activity
Review
Trends
Tips &
Issues

Issue 19

In Focus: Foreign Corruption

Published under the auspices of the BSA Advisory Group.

May 2011

Table of Contents

Introduction	1
Section 1 – Director’s Forum	3
Section 2 – Trends & Analysis	5
Summary Statistics of Corruption-Related SAR Filings.....	6
SARs Filed by Depository Institutions on Politically Exposed Persons.....	14
SAR Filings on Senior Foreign Political Figures and Foreign Corruption.....	16
Section 3 – Law Enforcement Cases	19
Section 4 – Issues & Guidance	29
A Compilation of FinCEN’s Anti-Corruption-Related Regulatory Efforts.....	29
General Regulatory Requirements Related to Corruption and PEPs.....	35
A View from Miami.....	40
Priorities and Initiatives of the Asset Forfeiture and Money Laundering Section, United States Department of Justice.....	43
Writing Effective SAR Narratives.....	46
Section 5 – Industry Forum	53
Challenges & Limitations of Identifying PEPs & Determining Relevant Risks.....	53
Who is a Politically Exposed Person: Challenges in Identifying PEPs.....	56
Politically Exposed Persons: Practical Considerations and Controls.....	62
Section 6 – Feedback Form	71

The *SAR Activity Review* **Index** is available on the FinCEN website at:

http://www.fincen.gov/news_room/rp/files/reg_sar_index.html

For your convenience, topics are indexed alphabetically by subject matter.

The **Archive of Law Enforcement Cases** published in *The SAR Activity Review* can be accessed through the following link:

http://www.fincen.gov/news_room/rp/sar_case_example.html

Introduction

The SAR Activity Review – Trends, Tips & Issues is a product of continual dialogue and collaboration among the nation’s financial institutions, law enforcement officials and regulatory agencies to provide meaningful information about the preparation, use and value of Suspicious Activity Reports (SARs) and other Bank Secrecy Act (BSA) reports filed by financial institutions.

This edition focuses primarily on foreign corruption, including identifying and reporting on suspicious activities involving senior foreign political figures. The *Trends & Analysis* section leads with an overview of corruption-related SAR filings covering 2009 and 2010, followed by articles that take a more focused look at two aspects of these filings.

The law enforcement cases in Section 3 demonstrate how important and valuable BSA data is to the law enforcement community. This section highlights a case involving foreign corruption, as well as domestic corruption cases, and illustrates how financial institutions have assisted in identifying instances of corruption through their BSA reporting.

In *Issues & Guidance*, we present two articles that discuss FinCEN’s efforts related to foreign corruption and regulatory expectations as they relate to foreign corruption. We also gain valuable feedback on SAR filings from a representative of Immigration and Customs Enforcement in *A View from Miami*. A representative from the Department of Justice’s Asset Forfeiture and Money Laundering Section also shares information on AFMLS’ priorities and initiatives, including their Kleptocracy Asset Recovery Initiative. Finally, we close this section with information for filers in writing effective SAR narratives.

In the *Industry Forum*, we get an industry viewpoint on the challenges and limitations in identifying politically exposed persons from three financial institutions – illustrating the similarities and differences that exist among institutions in addressing this aspect of their compliance programs.

You can subscribe to FinCEN Updates under “What’s New” on the FinCEN website, www.fincen.gov, to receive notification of when *The SAR Activity Review* is published. As always, we very much appreciate your feedback. Please take a moment to fill in the form in Section 6 to let us know if the topics we have covered are helpful to you, as well as what you would like to see covered in future editions. The form may be forwarded to FinCEN at the email address sar.review@fincen.gov. Please do not submit questions regarding suspicious activity reports to *The SAR Activity Review* mailbox.

Barbara Bishop
Regulatory Outreach Project Officer
Financial Crimes Enforcement Network

The SAR Activity Review is possible only as a result of the extraordinary work of many FinCEN employees and FinCEN’s regulatory, law enforcement and industry partners. FinCEN would also like to acknowledge the members of the Bank Secrecy Act Advisory Group (BSAAG) SAR Activity Review Subcommittee for their contributions to the development of this publication, particularly the Co-chairs noted below.

Lilly Thomas
Vice President and Regulatory Counsel
Independent Community Bankers of America

Helene Schroeder
Special Counsel
Commodity Futures Trading Commission

Section 1 — Director's Forum



For just over a decade, FinCEN has been publishing The *SAR Activity Review – Trends, Tips & Issues* as a resource for financial professionals, regulators, and law enforcement investigators. Our goal has always been to make the investment that we all have in SARs more effective, more efficient, and more valuable. This *Review* focuses on a topic that literally should be of concern to most of the people in the world, and where FinCEN's approach continues to play a major role in combating criminal activity: Corruption.

It is a sad truth that some degree of corruption occurs in both advanced and emerging economies, and that this illicit “tax” steals profits and productivity from every citizen and their respective governments. Those who hold positions of influence and power, or, in our generic anti-money laundering parlance, Politically Exposed Persons (PEPs), may be tempted to use their influence for personal gain. Whether it is a simple bribe to an official, or the siphoning of millions of dollars of oil revenue, almost all cases of corruption share a common trait: money -- sometimes in staggering amounts -- is moving.

When that money moves, FinCEN and its domestic and international network of partners are well positioned to follow the trail. FinCEN is the informational center of mass that attracts data from over a hundred thousand U.S. financial institutions and over one hundred counterpart Financial Intelligence Units (FIUs) located around the world, and we broadly share that centralized knowledge. Additional tools such as reaching out to financial institutions through the 314(a) program have added critical value in anti-corruption investigations. Support to individual investigations and prosecutions related to corruption are an important part of FinCEN's daily work.

Financial institutions are obviously on the front line of determining who is a PEP, what the risks are, and what transactions may involve the proceeds of corruption. As the authors note in the following *Industry Forum* section, this is a challenging, but extremely important, task. We often get questions and we attempt to provide solid guidance on how to evaluate these potential risks. This is further discussed in the

Issues & Guidance section. My personal experience invariably shows that financial institutions want to do the right thing. They want to use the powerful tools at hand, including Customer Identification Programs and customer due diligence, to provide quality information to help in the fight against financial crime and corruption. Several case examples are provided that demonstrate the ways that data reported to FinCEN by financial institutions is used. Many of the examples share a common phrase: the case was initiated by information provided by an “alert bank.”

The Egmont Group plays a powerful role in fighting corruption through preventing, detecting, and recovering the proceeds of this crime. International communication between individual FIUs adds unique value. The reason is simple -- many corrupt foreign officials will seek to launder or subsequently maintain illicit assets in countries away from home. Depending on the depth of corruption, the home country money trail may be entirely erased, or the accountability mechanisms themselves compromised. Working cooperatively, FIUs can track down these assets and share financial intelligence as lead information in the early stages of investigations, as well as subsequently seeking to recover stolen assets.

It is in all our interests to combat foreign corruption and to deprive corrupt officials’ access to international financial markets to launder diverted funds. It is also evident that victimized countries need the help of the United States and other foreign governments to track down and seek to return the proceeds of corruption to their rightful owners, the people of the country.

We hope that the information contained in this *Review* will add to our common base of shared knowledge and help improve both the quality of information provided by financial institutions and the investigatory utilization of that information.

James H. Freis, Jr.
Director
Financial Crimes Enforcement Network

Section 2 - Trends & Analysis

This section of *The SAR Activity Review - Trends, Tips & Issues* contains three related analyses of Suspicious Activity Reports filed by various industries related to senior foreign political figures and corruption.

Summary Statistics of Corruption-Related SAR Filings provides an overview of the characteristics of these reports. The Methodology and Explanation of Key Terms discussed in the first article also apply to the two subsequent articles in this section. The article *SARs Filed by Depository Institutions on Politically Exposed Persons (PEPs)* focuses on the subset of reports containing the commonly used term “politically exposed person” to determine the relationships between depository institutions and the persons to whom they refer as PEPs. *SAR Filings on Senior Foreign Political Figures and Foreign Corruption* provides a closer analysis of depository institutions SARs and SAR-SFs related to these specific terms.

The term “politically exposed person” (PEP) is commonly-used, especially in international fora. The term PEP is not included in FinCEN’s regulations and should not be confused with “senior foreign political figure.” By using the term PEP for ease of reference, FinCEN is seeking to more effectively discuss matters of corruption without continuous clarification of specific regulatory obligations based on customer types and products and services offered. The use of the term PEP in this document refers collectively to 1) the specific enhanced due diligence obligations for private banking accounts that are established, maintained, administered, or managed in the United States for senior foreign political figures, and 2) the general due diligence procedures required for all politically exposed persons, incorporated into the institution’s anti-money laundering program as appropriate.

Summary Statistics of Corruption-Related SAR Filings

By FinCEN's Office of Outreach Resources

Methodology

FinCEN analysts identified activity related to possible corruption by searching for keywords in the narratives of the depository institution Suspicious Activity Report (SAR), Suspicious Activity Report by the Securities and Futures Industries (SAR-SF)¹, Suspicious Activity Report by Money Services Businesses (SAR-MSB), and Suspicious Activity Report by Casinos and Card Clubs (SAR-C) filings between January 1, 2009 and December 31, 2010.

Explanation of Key Terms

Analysts searched narratives for the following terms: “senior foreign political figure²,” “foreign corruption,” “politically exposed person,” “PEP,” “kleptocrat,” and “kleptocracy.” Analysts screened the resulting filings from this search to eliminate false hits and references to the terms as part of a legal disclaimer. False hits fell into two categories: the search term was used as part of a phrase or business name unrelated to its meaning in this study (“pep rally”), or the term was used in a negative sense to indicate that certain activity was not occurring (i.e., the filer searched to see if the subject was a PEP and found no such evidence.) All figures presented in this *Trends & Analysis* section are exclusive of these types of filings.

Please note with respect to the discussion below that the number of subjects reported in SARs may not indicate the number of SARs filed, and that the number of SARs filed may not indicate the number of separate incidents reported. When a number is given on subjects originating from a specific state, for example, this number could represent ten financial institutions filing on ten different subjects or a single institution filing one SAR on ten subjects. Five filings may reflect for example the reporting of five separate incidents, or could represent the filing of SARs every 90 days on continuing activity.

1. SAR-SF filings include any related filings by insurance companies during the period for this study.
2. In BSA regulations, the term “senior foreign political figure” includes a current or former senior official of a foreign government or of a major foreign political party and a current or former senior executive of a foreign government-owned commercial enterprise. It also includes a corporation, business, or other entity that has been formed by, or for the benefit of, any such individual, the immediate family members of any such individual, and any person widely or publicly known, or actually known by the covered financial institution to be a close associate of any such individual. See 31 C F R. § 1010.605(p).

Findings

Descriptions of Reported Activities in SAR Narratives


Narratives of 1,294 discrete SARs contained one or more of the keywords. Filers used the terms “Politically Exposed Person” or “PEP” in 90.4%, “foreign corruption” in 9.6%, and “senior foreign political figure” in 5.0% of these filings. No filers used the terms “kleptocracy” or “kleptocrat.”

	SAR	SAR-SF	SAR-MSB	Total
Politically Exposed Person/PEP	1,094	68	8	1,170
Foreign Corruption	114	10	0	124
Senior Foreign Political Figure	58	7	0	65
Any term above ³	1,201	85	8	1,294

Top Filing Institutions

Depository Institution SAR

A total of 164 unique depository institutions⁴ filed SARs with one or more of the key terms in the narrative section. The top 5 of the 164 filers submitted 394 SARs, with each of these institutions submitting over 50 SARs.

SARs filed	# of institutions		Top 5 SAR Filers	Number Filed
51 +	5		Filer A	134
41 – 50	2		Filer B	72
31 – 40	3		Filer C	64
21 – 30	3		Filer D	63
11 – 20	9		Filer E	61
4 – 10	35			
1 – 3	107			

3. Several SAR narratives contained more than one of the terms. SARs with narratives containing more than one term are counted only once.
4. As identified by Filer Employer Identification Number/Social Security Number.

SAR-SF

A total of 23 unique institutions, either those in the securities and futures industries or insurance industry, filed the 85 SAR-SFs. The top 3 SAR-SF filers submitted 39 forms, with each institution filing at least 11 SAR-SFs.

Table 3: Top SAR-SF Filers

SAR-SFs filed	# of institutions		Top 3 SAR-SF Filers	Number Filed
11 +	3	➔	Filer A	15
4 – 10	6		Filer B	13
1 – 3	14		Filer C	11

SAR-MSB

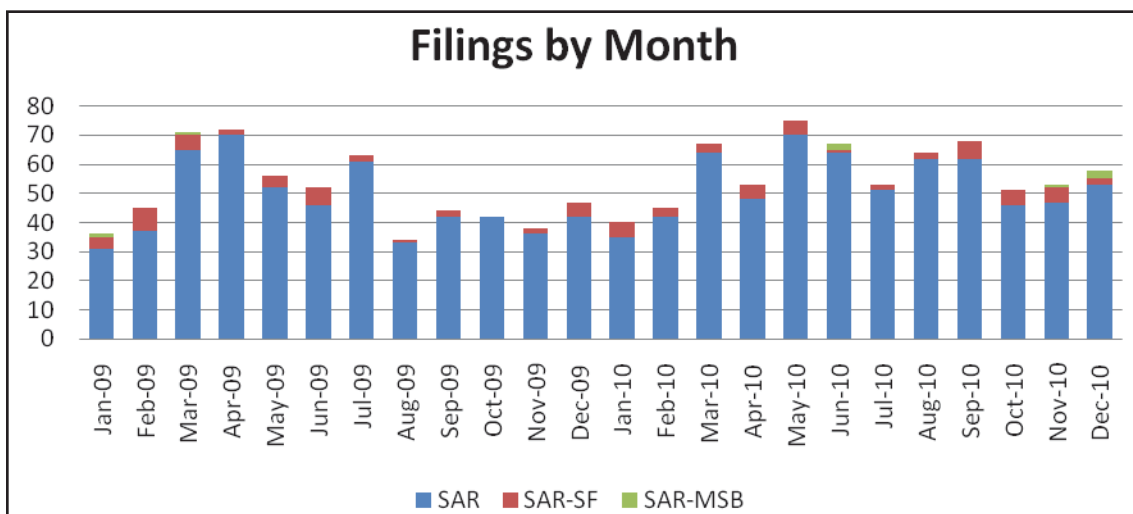
A total of 5 unique money services businesses filed SAR-MSBs with the key terms.

Table 4: SAR-MSB Filers	
All MSB-SAR Filers	Number Filed
Filer A	2
Filer B	2
Filer C	2
Filer D	1
Filer E	1

Total SAR Filings by Month

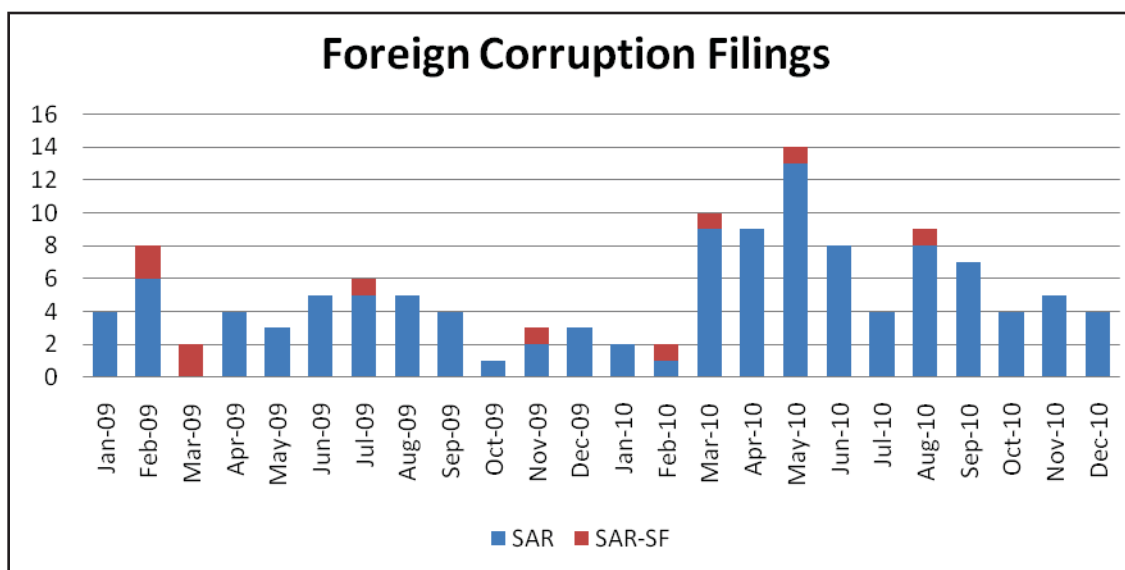
Graph 1 indicates the number of SARs filed in 2009 and 2010.

Graph 1



Graph 2 shows filing dates only for depository institution SARs and SAR-SFs with narratives that contain the term “foreign corruption.” This graph demonstrates a rise in filings after February 2010. Note that the U. S. Senate Permanent Subcommittee on Investigations published its staff report, *Keeping Foreign Corruption Out of the United States: Four Case Histories*⁵ on February 4, 2010. FinCEN Director Freis testified before the Subcommittee at a hearing discussing that report.⁶

Graph 2



Institutions are required to file a SAR not later than 30 calendar days after the date of initial detection of facts that may constitute a basis for its filing. If no subject is identified on the date of such initial detection, an institution may delay filing for an additional 30 calendar days.

5. See http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=999271b5-e1b2-4ef3-944b-e687f52ee557.

6. See http://www.fincen.gov/news_room/testimony/html/20100204.html

Table 5 shows quartiles for the number of days between the date when suspicious activity began⁷ and date the institution filed the SAR.

Table 5: Activity versus Reporting Dates			
	SAR	SAR-SF	SAR-MSB
First Quartile	109	78	21
Second Quartile	224	306	87
Third Quartile	576	720	435
Minimum	0	5	0
Maximum	4,186	2,712	964

Subject Location

Filers reported subject addresses located in 125 countries including the United States. Within the United States, institutions reported subject addresses in 44 states, the District of Columbia and Puerto Rico.

Table 6: Subject Address Locations	
Top 10 Locations⁸	Subject Count
New York	156
Florida	138
California	127
Texas	85
Virginia	64
Maryland	44
Michigan	42
District of Columbia	33
New Jersey	28
Illinois	19
Georgia	19

7. As reported in Part III, Field 33, in the depository institution SAR, Part II, Field 21 in the SAR-SF, and Part II, Field 16 in the SAR-MSB.

8. Illinois and Georgia tied for 10th with 19 subjects reported.

Dollar Amounts Involved in Reported Activities

Institutions reported a wide range of total dollar amounts involved in reported activities. Note that the dollar amounts presented here cannot necessarily be attributed to foreign corruption or to specific actors. For example, an institution may have reported on activities that involved a total of \$10 million, of which a single \$1,000 transaction involved a politically exposed person. Furthermore, some SARs reported ongoing activity described in a previous SAR within the data; the amount reported on the most recent SAR would reflect both new activity amounts and amounts also reported on the older SAR(s). Finally, some SAR filers did not include a dollar amount of the suspicious activity.⁹

Table 7: Suspicious Activity Dollar Amounts			
<i>Total dollar amounts involved</i>	SAR	SAR-SF	SAR-MSB
\$0-\$5,000.00	33	5	2
\$5,000.01 – \$100,000.00	383	17	4
\$100,000.01 - \$500,000.00	341	19	2
\$500,000.01 - \$1,000,000.00	111	4	–
\$1,000,000.01 - \$10,000,000.00	211	28	–
\$10,000,000.01 - \$50,000,00.00	52	7	–
\$50,000,000.01 - \$100,000,000.00	12	2	–
\$100,000,000.01 and over	28	3	–
Amount left blank	30	–	–

Suspicious Activity Characterizations

Depository Institution SAR

Of the 1,201 SARs filed by depository institutions in the two-year study period, 1,103 (91.84%) listed “Bank Secrecy Act/Structuring/Money Laundering” as a characterization of suspicious activity. For the period April 1, 1996 through June 30, 2010, BSA/Structuring/Money Laundering was selected in 46.39% of all filings by depository institutions.¹⁰ One-hundred ninety-seven SARs (16.40%) listed the characterization “Other,” as compared to 9.50% of all depository institution filings for the period April 1, 1996 through June 30, 2010. Within this group, “Other” was

9. Part III, Field 34 in the depository institution SAR, Part II, Field 22 in the SAR-SF, and Part II, Field 17 in the SAR-MSB.

10. See *The SAR Activity Review – By The Numbers* Issue 15 (January 2011) http://www.fincen.gov/news_room/rp/files/sar_by_num_15.pdf.

the only characterization checked in 77 SARs. Common descriptions of this activity included variations on the following: unusual/suspicious wire activity, negative information found, and unlicensed currency exchange.¹¹

Table 8: Suspicious Activity Characterizations Reported in Depository Institution SARs		
Characterization of Suspicious Activity – Part III, Field 35	Number of Occurrences	Percentage
Bank Secrecy Act/Structuring/Money Laundering	1,103	91.84%
Bribery/Gratuity	10	.83%
Check Fraud	2	.17%
Commercial Loan Fraud	2	.17%
Computer Intrusion	1	.08%
Counterfeit Instrument (other)	1	.08%
Credit Card Fraud	4	.33%
Defalcation/Embezzlement	7	.58%
False Statement	10	.83%
Misuse of Position or Self Dealing	7	.59%
Mortgage Loan Fraud	3	.25%
Wire Transfer Fraud	14	1.17%
Other	197	16.40%
Terrorist Financing	7	.58%
Identity Theft	1	.08%
Characterization left blank	4	.33%

SAR-SF

Of the 85 SAR-SF filings, 43 (50.59%) listed “Money Laundering/Structuring” as the type of suspicious activity. This characterization was listed in 15.47% of all filings on this form for the period of January 1, 2003 through June 30, 2010. Forty SAR-SFs (46.06%) listed “Significant wire or other transactions,” as compared to only 8.18% of the filings for the period of January 1, 2003 through June 30, 2010.

11. Note that filers may mark multiple types of suspicious activity in one SAR. Therefore, the number of activities may exceed the number of filings and total percentages for all characterizations may exceed 100%.

Table 9: Suspicious Activity Characterizations Reported in SAR-SFs¹²

<i>Type of Suspicious Activity Part II – Field 30</i>	<i>Number of Occurrences</i>	<i>Percentage</i>
Bribery/gratuity	3	3.53%
Embezzlement/theft	2	2.35%
Insider trading	2	2.35%
Market manipulation	2	2.35%
Money laundering/Structuring	43	50.59%
Securities fraud	3	3.53%
Significant wire or other transactions without economic purpose	40	47.06%
Suspicious documents or ID presented	8	9.41%
Wire fraud	2	2.35%
Other	27	31.76%
Type of suspicious activity left blank	1	1.18%

SAR-MSB¹³**Table 10: Suspicious Activity Characterizations Reported in SAR-MSBs¹⁴**

<i>Category of Suspicious Activity Part II – Field 18</i>	<i>Number of Occurrences</i>
Money laundering	4
Other	4
(blank)	1

12. Ibid.

13. Ibid.

14. Ibid.

SARs Filed by Depository Institutions on Politically Exposed Persons (PEPs)

By FinCEN's Office of Outreach Resources

This article focuses solely on depository institution SARs filed in 2009 and 2010 with narratives that contained either “politically exposed person” or “PEP,” a subset of data identified in the previous article, *Summary Statistics of Corruption-Related SAR Filings*.

	SAR	SAR-SF	SAR-MSB	Total
PEP/Politically Exposed Person	1,094	68	8	1,170
Foreign Corruption	114	10	0	124
Senior Foreign Political Figure	58	7	0	65
Any term above	1,201	85	8	1,294

The predominant use by depository institutions of “politically exposed person” (1,094 SARs) over “senior foreign political figure” (58 SARs) is particularly notable, because only the latter term is defined in FinCEN’s regulations. This statistic may not be surprising, however, given the use of the former term in international fora and, perhaps more importantly, its use by vendors of commercial lists. In this article, we more closely analyze the relationships between depository institutions and the persons to whom they refer as PEPs. To this end, FinCEN analysts selected a random sample of 300 SARs from among the group of 1,094 for closer review.

Customers

Depository institutions used the term “politically exposed person” or “PEP” in reference to their own customer in roughly half of the 300 SARs. The filings within this group largely tell three different stories.

The majority of SAR filings appeared to report on activities of customers the financial institution knew to be politically exposed persons.

In about two dozen SARs, the financial institution reported that an investigation, internet research or a search of a commercial database revealed the name of a politically exposed person which matched that of the customer; however, the institution was either unable to confirm whether the customer was in fact the PEP, or

believed that the hit was false based on other identifying information. Some of these narratives listed the PEP match among many possible hits for the individual within a database. In a handful of SARs, the narratives did not specify whether and how the financial institution resolved the potential PEP designation of its customer.

There were about 20 filings in which the financial institution appeared to learn that its customer may be a politically exposed person during the course of an investigation. A few of these specifically stated that the account would be considered a PEP account or identified for enhanced monitoring. These SARs highlighted the utility of the investigation process as a point at which a financial institution may obtain information that would lead to the classification of a customer as a PEP, especially when the information was not otherwise known through the financial institution's account opening procedures or ongoing risk-based monitoring.

Product lines used by PEP customers

Narratives noted PEP customers using a variety of account products, including personal checking, business checking, money market, and personal savings. While some of these may have been private banking accounts¹⁵, only a handful of SARs affirmatively noted that the financial institution was filing on a PEP customer for whom it maintained a private banking relationship. The article *A Compilation of FinCEN's Anti-Money-Related Regulatory Efforts* in the *Issues & Guidance* section includes a discussion of the regulatory requirements for private banking accounts.

Counterparties to transactions with customers

Depository institutions used the term "politically exposed person" or "PEP" in reference to the counterparties of transactions with their customer in about a third of the SARs. Most of these SARs identified the counterparty as a match or possible match to a PEP found through internet research or listed in a commercial database, generally discovered during an investigation into the suspicious activity. This PEP match was often one of among many possible matches for the individual noted in the

15. A "private banking account" is defined in 31 CFR 1010.605(m) as an account (or any combination of accounts) maintained at a covered financial institution that: (1) requires a minimum aggregate deposit of funds or other assets of not less than \$1,000,000; (2) is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account; and (3) is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of a covered financial institution acting as a liaison between the covered financial institution and the direct or beneficial owner of the account.

narrative, and the individual was often involved in only one of many transactions with the customer. The filer initiated these investigations due to a variety of reasons, among them large incoming wire transfers from countries designated as high risk by the financial institution, and unusual cash deposits/structuring.

There were about a dozen SARs in which it appears that the financial institution was alerted to the suspicious activity through searches for the PEP counterparty following media coverage of potential corruption.

Correspondent banking

Approximately one sixth of the reports within the sample, filed by 16 unique depository institutions, used the term “PEP” in reference to activity occurring in correspondent accounts maintained for foreign financial institutions. These referenced the PEP status or possible PEP status of both the customer of the correspondent bank (the customer’s customer), and counterparties to these transactions. In several instances, it appears that the financial institution’s search for the specific PEP within their correspondent account activity led to the identification of suspicious activity.

SAR Filings on Senior Foreign Political Figures and Foreign Corruption *By FinCEN’s Office of Outreach Resources*

This article focuses on the subset of filings whose narratives contained the term “senior foreign political figure” or “foreign corruption.” Because these terms appeared in a relatively small number of filings, analysts were able to examine every SAR that contained either term. For this article, we treat SARs using these two terms as two different groups of filings; SARs that contained both terms are included in both groups.

	SAR	SAR-SF	SAR-MSB	Total
PEP/Politically Exposed Person	1,094	68	8	1170
Foreign Corruption	114	10	0	124
Senior Foreign Political Figure	58	7	0	65
Any term above	1,201	85	8	1,294

Filing institution's relationship to involved parties

Within the SARs which contained only the term “foreign corruption,” analysts identified the actor(s) who could be most closely characterized as a senior foreign political figure or PEP, or the entity most likely to be under the control of the senior foreign political figure or PEP. Such identified actors were the customers of the filing institution in 40 SARs within the “foreign corruption” group, and non-customer counterparties to a transaction in 51 SARs. The corresponding numbers for the “senior foreign political figures” group were 35 filings and 24 filings, respectively.

Where these actors were natural persons, about half could be considered politically exposed persons due to a position they held when or prior to the time the SAR was filed, and the other half through a relationship to a family member or a close association to a senior foreign political figure or PEP.

Twenty-two SARs (17.7%) referenced correspondent banking in the “foreign corruption” group, as did two filings in the “senior foreign political figure” group. Similar to filings containing the term “politically exposed person,” very little activity was affirmatively attributed to private banking.

Accountholder addresses

Analysts also examined narratives to determine the residential or other location of the financial institution's customer (but not necessarily the PEP). Within the “foreign corruption” group, 72 filings (58.1%) described a customer living in the United States, while 35 SARs (28.2%) reflected either a customer living abroad or foreign-based wire counterparties or customers of correspondent banks. In the “senior foreign political figure” group, 36 SARs (55.4%) noted a customer living in the United States and 24 SARs (36.9%) indicated either a customer living abroad or foreign-based wire counterparties or customers of correspondent banks.

Foreign Corrupt Practices Act

In both the “foreign corruption” and “senior foreign political figure” groups, few filers explicitly noted activity in possible violation of the Foreign Corrupt Practices Act. A more comprehensive study of such activity would need to include more terms relevant to this specific issue.

Shell Entities

Analysts identified 24 SARs (19.3%) in the “foreign corruption” group and 6 (9.2%) in the “senior foreign political figures” group in which the filer reported that it suspected that shell entities played a role in the suspicious activity.

The SAR narratives did not usually specify whether a named company was an operational entity engaged in business activities, unless the filer explicitly noted this not to be the case; filers did not tend to state that a company was suspected or known to be operational, which could reflect either that they did not have this information or that they did not find it noteworthy in a description of suspicious activity.

Conclusion

Taken together, the preceding three articles can provide a foundation for discussions on regulatory expectations related to politically exposed persons. *Summary Statistics of Corruption-Related SAR Filings* offers a summary of the SAR filings based on the fixed fields on the forms, including the number of filing institutions using specific terms, the characterizations of suspicious activity, subject locations, and the dollar amounts involved. These statistics illuminate the scope of issues discussed in more detail later in this edition.

SARs Filed by Depository Institutions on Politically Exposed Persons and *SAR Filings on Senior Foreign Political Figures and Foreign Corruption* focus on the financial products used by politically exposed persons, as well as on how the filer learned that parties involved in suspicious activity might be PEPs. Such information is useful for discussions of regulatory expectations of risk-based approaches to the identification and monitoring of PEP customers.

Section 3 – Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where BSA information played an important role in the successful investigation and prosecution of criminal activity. This issue contains new case examples from Federal and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website under the link to Investigations Assisted by BSA Data. This site is updated periodically with new cases of interest.

Contributing editors: Shawn Braszo, Vanessa Morales, James Emery, Nivine Hanna, and Jack Cunniff.

In this edition of *The SAR Activity Review*, we include cases where public officials either pleaded guilty or were convicted at trial on corruption charges or other illegal activity. Our first case involves foreign corruption, while the rest focus on individuals in a position of public trust in the United States who abused their position for personal gain, or otherwise engaged in criminal acts. The defendants range from local elected officials, to State and Federal employees, and employees of public utilities. The common feature of these investigations is that BSA records, particularly SARs, played a significant role in the successful investigation and prosecution of the defendants, and illustrate how financial institutions have assisted in identifying instances of both foreign and domestic corruption through their BSA reporting. Oftentimes, it was the existence of requirements under the BSA, especially the reporting requirements for large currency transactions, which caused the defendants to alter their behavior and trigger additional scrutiny by financial institutions.

SAR Leads to Recovery of Funds Derived From Foreign Corruption

An alert financial institution, upon learning of negative information on potential clients, filed a SAR and notified Federal law enforcement officials of its findings. The ensuing investigation revealed that several subjects conducted a complex series of transactions, over a period of several years, using the proceeds of foreign

corruption. Many of those transactions were funneled through the United States' financial system. Ultimately, Federal officials seized and forfeited criminal proceeds valued at more than \$100 million.

The investigation centered on the circumstances surrounding a foreign civil case in which the judge found for the plaintiff and ordered the defendant to pay the plaintiff (and heirs) the U.S. equivalent of half a billion dollars. Soon after the judgment in the civil case, law enforcement commenced an investigation into the possibility that the decision in the civil case was the result of a bribe, worth tens of millions of dollars, paid to the judge through a group of attorneys. This investigation led to the arrest of several individuals involved in the civil case, including the plaintiff's heir, the judge and the attorneys. The judge and the attorneys were convicted of bribery.

During the 10-year period over which the suspicious activity was occurring, a financial advisor, working in conjunction with other heirs of the plaintiff, engaged in a conspiracy to launder millions of dollars derived from the bribery scheme. After the bribery scandal broke, the advisor helped set up corporate and trust structures to conceal large portions of the public corruption proceeds. The evidence revealed that the advisor set up discretionary common law trusts, with the plaintiff's family members named as beneficiaries, leading to the creation of shell companies and other entities to hold the assets for the trusts. A significant portion of the public corruption proceeds were then moved through these entities to or through bank and investment accounts located in the United States. The advisor was listed as a signatory to accounts held in the names of companies that he created to hold the stolen funds – which were assets of the trusts he controlled to conceal the true beneficial owner of the funds.

Through the cooperative efforts of U.S. and foreign investigators, the funds were traced through a vast array of accounts in multiple jurisdictions and through corporate and trust structures. Investigators were able to establish links between the bribery proceeds and numerous bank and brokerage accounts located on the East and West coasts of the United States, which were ultimately seized.

Eventually, all family heirs associated with the theft were arrested, pleaded guilty, and were sentenced to prison. The financial advisor was arrested. U.S. authorities became involved when some of the heirs attempted to open accounts in the United States. Through the use of BSA data, especially SARs, and investigative information provided by foreign authorities, investigators identified approximately 2 dozen accounts in the United States that contained the proceeds of the fraud and bribery scheme.

Proactive SAR Review Leads to the Arrest of Army Officer and Recovery of Iraqi War Funds

A U.S. military officer used his official position to steal currency designated for war use, transferred the funds to the United States, and then spent that money on personal items. When the defendant conducted transactions with the stolen currency at financial institutions, those transactions triggered anti-money laundering detection protocols. The resulting SAR led to a quick arrest and recovery of the stolen currency.

This is an example where the underlying crime went undetected, but where BSA reporting requirements resulted in the identification of transactions involving the fruits of the crime. The facts of the case stated that for a period of almost 2 years, the defendant was deployed to Iraq and was responsible for making monthly payments in U.S. currency, derived from an emergency relief program, to Iraqi nationals. At any one time, the defendant had nearly \$300,000 in cash locked in a safe.

During his deployment, the defendant stole nearly \$700,000 of the funds, which consisted of newly issued \$100 bills. The defendant then forwarded the currency to his home address before returning from Iraq. After returning home, the defendant opened accounts at several different depository institutions and began to deposit the stolen currency into the accounts. In a 3-month period, the defendant made numerous currency deposits on consecutive days or the same day for less than \$10,000. In all, the defendant deposited more than \$350,000 in stolen currency into the accounts.

With the stolen money in the accounts, the defendant proceeded to purchase cashier's checks for tens of thousands of dollars. The defendant used the checks to purchase expensive vehicles, electronics, computers, furniture, and handguns. Eventually a financial institution filed a SAR on some of the transactions. Of note, the SAR described a series of cash deposits on consecutive days or on nearly consecutive days where the source of the funds could not be determined and the aggregate amount exceeded reporting requirements.

An IRS agent conducted a proactive review of SARs and opened an investigation. Within a few months, agents executed a search warrant and found approximately \$300,000 in currency at the defendant's residence. The currency was still in the original wrappers from the Bureau of Engraving and Printing. Agents also seized around \$50,000 from bank accounts and approximately \$100,000 in investment accounts. Investigators, through either seizures or asset recovery, accounted for nearly all the stolen money.

A federal jury sentenced the defendant to several years in prison for structuring of financial transactions, theft of government property, and money laundering.

Casino Currency Transaction Reports Help Track Funds Embezzled from a Public Utility

A man with a compulsive gambling addiction embezzled millions of dollars from a public utility and lived the life of a “high roller” for several years before being caught. The defendant established several shell corporations to bilk a county for water well capacity rights.

As part of the investigation, investigators queried the BSA database and discovered more than 100 Casino CTR filings on the defendant. The records, which were filed over a period of 2 ½ years, included transactions in amounts of more than \$70,000 and helped investigators determine the disposition of the stolen funds.

The defendant admitted to a scheme in which he created dummy companies with corresponding bank accounts and falsified documents for the companies’ sales to the county of bogus water well capacity rights. The stolen money was from a water utility fund comprised of payments received from thousands of ratepayers and developers. The defendant gambled away most of the stolen money at local casinos where he enjoyed the perks of a high roller.

In a news release, the district attorney said that upon being alerted last year of the embezzlement, he and a sheriff’s detective began working to freeze the defendant’s bank accounts and search his home. Investigators found a stash of nearly \$8,000 in a suitcase in the defendant’s home.

A judge sentenced the defendant to 10 to 30 years in prison and ordered him to pay more than \$2 million in restitution.

Suspicious Activity Report Lead to Arrest and Conviction of U.S. Government Employee for Embezzlement

In a case initiated from a SAR review team, a Federal government accountant pleaded guilty to theft of public money and money laundering. The case began when an alert bank noticed several unusual transactions, including large cash payments to credit card accounts. Activity in one account at the bank, ostensibly a business account, appeared suspicious, because the only deposits were U. S. Treasury checks, most of the debits were for currency, and there was no apparent business activity.

A bank filed a SAR on the defendant indicating structuring and unusual transactions involving the subject's business. The SAR narrative revealed cash payments made to two credit card accounts of approximately \$8,000 each, but the balances on the cards were less than \$200. The bank reported several check deposits into the business account, with almost all of the withdrawals consisting of currency. In addition, the bank found no signs of checks drawn on the business account for business expenses.

The bank also noted that some of the cash withdrawals appeared to occur at casinos. The defendant received cash advances at casinos and sent some of those payments back to credit card accounts. Casinos filed more than 80 Currency Transaction Reports on the defendant beginning around the time the defendant began his embezzlement. In addition, a casino filed a SAR on the defendant for cashing nearly \$6,000 worth of checks in a month with no subsequent buy-ins or rated play.

The defendant confessed to creating a fictitious business along with creating more than a dozen government refund payment vouchers made payable to his business entity and directing the checks to be deposited into accounts of that entity. The defendant pleaded guilty to money laundering related to the financial transactions involving funds that were derived from the embezzlement.

A federal judge sentenced the defendant to more than 3 years in federal prison without parole. The court also ordered him to pay approximately \$600,000 in restitution.

Suspicious Activity Reports Identify Transactions Linked to Embezzlement of a Tribal Authority

A U.S. district judge sentenced a financial manager to 10 years in custody for using two financial institutions to launder funds from an embezzlement he orchestrated while working for an Indian tribal government entity receiving Federal funds. He was charged with stealing more than \$180,000 over a 2-year period. The defendant conducted a series of transactions, predominantly check cashing, that the banks believed to be designed to evade reporting requirements. The institutions filed SARs on the defendant, and these records proved very helpful to the investigation.

The case against the defendant began while investigators were looking into improper payments to a developer. The theft charges stem from a relationship that the defendant developed with the owner of a defunct retail store. The defendant would make phony payments to the store, which were in turn funneled back to him.

State and federal law enforcement agencies in two states opened concurrent investigations into the activities of the defendant. Interagency cooperation facilitated the investigation, and numerous BSA filings, particularly SARs, helped investigators to track the defendant's financial transactions over several years.

The defendant has a long history of transactions that resulted in SAR filings. Several years earlier, a bank reported that the defendant made a series of cash deposits that ranged from \$500 to more than \$10,000. When the bank asked him about the deposits, he stopped coming into the branches. Later, the bank filed additional SARs noting that the activity was continuing. None of these SARs noted any legitimate business activity.

In addition, the bank filed a SAR on the defendant for numerous cash-out transactions. In a 2-month period, the defendant withdrew nearly \$20,000 in cash. Moreover, the bank noted that in a 3-year period, the defendant received nearly \$90,000 in suspicious ACH deposits. The bank filed a subsequent SAR noting more than \$25,000 in additional suspicious cash withdrawals.

Another bank filed a SAR on the defendant and on a lending business completely controlled by the defendant and his wife. A review of the account revealed that during part of the year the defendant was responsible for cashing checks several times a week. During the reporting period, the defendant cashed nearly 40 checks in amounts ranging from \$1,500 to \$10,000 for a total of nearly \$260,000. The bank could not find any legitimate business purpose for the transactions, and believed the checks were structured to evade reporting requirements. The following year, the same bank filed a supplemental SAR describing nearly three dozen additional transactions for approximately \$230,000.

Corrupt Official Convicted on Numerous Charges Including Structuring

In a case where a corrupt politician extorted money from his constituents, investigators examining his financial records found numerous instances of structuring. In fact, three different banks filed SARs on the defendant detailing unusual transactions. Prosecutors charged the official with multiple counts of structuring and other crimes.

The official extorted three individuals in his district to pay him nearly \$100,000 in exchange for his support of zoning variances on properties. The jury also found that the defendant structured certain financial transactions in order to evade reporting requirements on several occasions. When the defendant demanded extortion money from victims, he claimed that he needed to share the money with his fellow elected officials to ensure the measures passed.

Over the course of several years, SARs were filed on the defendant. One bank filed a SAR for transactions that appeared to be structured while the defendant was in office. Bank personnel became concerned after discovering deposits that aggregated to several hundred thousand dollars. No single deposit exceeded \$10,000. A second bank filed a SAR on check cashing activity that aggregated to \$15,000 over successive days in an apparent attempt to avoid a Currency Transaction Report. A third bank filed several SARs based on transactions the defendant and a business associate conducted over 3 months, totaling over \$400,000.

The elected official was convicted of extortion, wire fraud, failure to file income tax returns, and multiple counts of structuring financial transactions.

Credit Union's Suspicious Activity Reports Lead to Arrest of Corrupt Utilities Employees

In a case that started with the discovery of structuring at a local credit union, investigators found corruption and kickbacks on the part of public transit and utilities officials. With some corrupt officials asking for a percentage in kickbacks on multi-million dollar contracts, the contractors and officials found themselves struggling to handle the currency that the scheme was generating. Multiple court documents describe conversations the defendants had about avoiding Bank Secrecy Act reporting requirements.

The case began when a task force identified several SARs filed on an employee of a utility company. The employee conducted a number of transactions, namely structured cash withdrawals, at a local credit union. The subsequent investigation determined that the employee was receiving kickbacks from various contractors. Further investigation uncovered the kickbacks paid to other utility employees.

The defendants in many instances approved payments for work that was never performed. In addition, the defendants often demanded as a kickback a percentage of the "extras," or unearned payments made to the contractor. Certain defendants demanded monthly kickback payments in exchange for ensuring that the contractor's invoices would be paid promptly, and that the payments requested in the invoices would not be cut. On other occasions, certain defendants agreed, in exchange for bribe payments, to direct additional work to the contractor that was not necessary or required.

In all, more than 10 individuals have pleaded guilty to charges related to soliciting and accepting more than \$1 million in kickbacks from a contractor in connection with construction projects.

Local Official Sentenced For Tax Evasion and Structuring

An elected official structured transactions in an attempt to disguise from the IRS his earnings from personal businesses. Investigators discovered the structuring after reviewing SARs filed by banks that detailed the illicit transactions.

The official operated a retail business and law firm. He failed to pay employment taxes based on his operation of the retail business, and then began to engage in more aggressive tax evasion, filing an income tax return disclosing an income tax liability of more than \$20,000 that he subsequently failed to pay. He also began a pattern of failing to pay employment taxes for his law firm as well.

The official began structuring the deposit and withdrawal of attorney's fees into and out of his law firm's escrow account and maintained only minimal amounts of money in the firm's operating account in an effort to prevent the IRS from determining his ability to pay the taxes he owed. In a 2-year period, the official structured almost \$300,000. When investigators reviewed the SARs, they were quickly able to outline numerous structuring transactions.

The official eventually pleaded guilty to tax evasion and structuring. A federal judge sentenced the official to just over 1 year in prison, to be followed by a 3-year supervised release, and ordered payment of tens of thousands of dollars in taxes, interest, and fines.

SARs Help Uncover Bid-Rigging Scandal

In a case where political corruption led to bid rigging of public housing contracts in order to defraud the government, BSA records proved instrumental in understanding the scheme. In this case, perpetrators repeatedly structured financial transactions in order to hide business relationships and launder funds.

A contractor won a federal grant for more than \$50 million for the demolition of a public housing development to construct new housing after a local elected official intervened on his behalf. The contractor's business was obligated to take legitimate competitive bids from other contractors seeking to provide demolition, earthwork, utilities, and concrete services. However, the contractor manipulated the bidding process used to select the primary contractor by creating false and fraudulent documents. He recruited and directed other companies to submit inflated bids in order for another one of his companies to appear to be the lowest bidder. The cooperating companies in return received sub-contracts and kick-backs for their false bids.

The contractor's businesses earned over \$10 million from the project. From those funds, he issued a check for over \$250,000 to a third company he owned. Over a period of several months, the contractor cashed more than a dozen separate checks issued to him from the company for a total of more than \$170,000. A SAR indicated that the transactions were structured to avoid CTR reporting requirements. The investigation was initiated after a government employee reported his suspicions of bid rigging to the Housing and Urban Development's Office of Inspector General.

The BSA information accessed on the contractor was instrumental in outlining his true relationships with the various businesses he in fact owned. Eventually some funds extracted from the scheme went to the elected official's campaign coffers.

The contractor and several co-defendants were indicted on numerous charges including conspiracy to defraud the government, mail fraud, money laundering, willfully injuring U.S. property, felon in possession of a firearm, obstruction of justice, and structuring.

Section 4 – Issues & Guidance

This section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of SARs and provides meaningful guidance to filers.

A Compilation of FinCEN’s Anti-Corruption-Related Regulatory Efforts

By FinCEN’s Office of Outreach Resources

FinCEN’s work in combating the flow of proceeds of foreign corruption into the United States is based on the three components of the U.S. domestic approach to combating foreign corruption, each benefitting from and helping to advance efforts to combat money laundering and other forms of illicit finance more broadly. These are:

- Requiring financial institutions to identify and apply enhanced due diligence to private banking accounts held by or for the benefit of senior foreign political officials, commonly referred to as Politically Exposed Persons (PEPs);
- Attuning U.S. financial institutions to risks, and providing guidance with respect to suspicious activity reporting requirements, regarding potential corrupt activity; and,
- Promoting the transparency of U.S. legal entities that may otherwise mask foreign corrupt activities of senior foreign political figures in the financial system.¹⁶

16. Statement of FinCEN Director James H. Freis, Jr. before the United States Senate Committee on Homeland Security and Government Affairs Permanent Subcommittee on Investigations, February 4, 2010, at http://www.fincen.gov/news_room/testimony/html/20100204.html.

Section 312 and Implementing Regulatory Requirements

The goal of Section 312 of the USA PATRIOT Act is to deter attempts to launder money through correspondent and private banking accounts.¹⁷ Specifically, Section 312 imposes due diligence and, in some cases, enhanced due diligence, with regard to correspondent accounts¹⁸ established, maintained, administered, or managed in the United States for foreign financial institutions, and private banking accounts established, maintained, administered, or managed in the United States for non-U.S. persons.

Foreign Correspondent Banking

The ability of corrupt foreign financial institutions to transact business in the United States,¹⁹ and the ability of customers of a lax foreign correspondent to access the U.S. financial system through the correspondent account while shielding their identities, were two concerns that led to the promulgation of Section 312.²⁰ U.S. financial institutions are required under FinCEN's rules implementing Section 312 to apply due diligence to correspondent accounts for foreign financial institutions.

Enhanced Due Diligence Requirements

Section 312 contains a provision requiring U.S. financial institutions to apply enhanced due diligence when establishing or maintaining a correspondent account for a foreign bank that is operating under an offshore license, or located in a jurisdiction found to be non-cooperative with international anti-money laundering principles, or located in a jurisdiction found to be of primary money laundering concern.²¹

17. See 147 Cong. Rec. S10990, 11035 (Oct. 25, 2001) (Statement of Senator Carl Levin (D-MI)).

18. A correspondent account includes any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution. While this is a relatively broad definition, it does require a formal relationship through which the financial institution provides regular services.

19. See Minority Staff Report on Correspondent Banking: A Gateway to Money Laundering: Hearing Before the Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 107th Cong., 277–884 (2001).

20. See Section 302(a)(6) of the USA PATRIOT Act (finding that “correspondent banking facilities are one of the banking mechanisms susceptible in some circumstances to manipulation by foreign banks to permit the laundering of funds by hiding the identity or real parties.”)

21. Section 311 of the USA PATRIOT Act, which establishes procedures for FinCEN to follow, and factors for FinCEN to consider, when determining that a jurisdiction outside the United States is of primary money laundering concern.

With regard to correspondent accounts for such banks, U.S. financial institutions must take reasonable steps to: (1) conduct appropriate enhanced scrutiny; (2) determine whether the foreign bank itself offers correspondent accounts to other foreign banks (i.e., nested accounts) and, as appropriate, identify such foreign bank customers and conduct additional due diligence on them; and (3) identify the owners of such foreign bank, if its shares are not publicly traded. Financial institutions have flexibility in applying the enhanced due diligence procedures, using a risk-based approach and tailoring it to the risks associated with a particular account.²²

Private Banking

Private banking accounts²³ may be particularly vulnerable to money laundering, to the extent they may afford wealthy clients a large measure of anonymity.²⁴ As with correspondent accounts, U.S. financial institutions covered by the private banking rule are required to establish and maintain a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving private banking accounts.

Specifically, financial institutions must take reasonable steps to: (1) determine the identity of all nominal and beneficial owners of the private banking account; (2) determine whether any such owner is a senior foreign political figure and, thus, is subject to enhanced scrutiny (described below); (3) determine the source(s) of funds deposited into the private banking account and the purpose and expected use of

-
22. Specifically, regulations implementing Section 312 provide that enhanced scrutiny shall reflect the risk assessment of the account and shall include, as appropriate: (i) Obtaining and considering information relating to the foreign bank's anti-money laundering program to assess the risk of money laundering presented by the foreign bank's correspondent account; (ii) Monitoring transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity; and (iii) Obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account, and the sources and beneficial owner of funds or other assets in the payable-through account.
 23. Significantly, if an account otherwise satisfies the definition of a private banking account as described above, but the institution does not require a minimum balance of \$1,000,000, then the account does not qualify as a private banking account under the private banking rule. However, the account is subject to the internal controls and risk-based due diligence included in the institution's general anti-money laundering program.
 24. See Hearings on Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities, Before the Permanent Subcommittee on Investigations of the Senate Committee On Governmental Affairs, 106th Cong., 872 (1999) (Minority Staff Report).

the account; and (4) review the activity of the account to ensure that the activity is consistent with the information obtained about the source of funds, the stated purpose and the expected use of the account, as needed to guard against money laundering, and to report any suspicious activity.

Enhanced Due Diligence

Included in the rule for private banking accounts is a duty to conduct enhanced scrutiny of private banking accounts maintained for senior foreign political figures. The enhanced scrutiny must include procedures reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

Senior Foreign Political Figures

A “senior foreign political figure” is defined as: a current or former senior official of a foreign government, whether elected or not; a senior official of a major foreign political party; and a senior executive of a foreign government-owned commercial enterprise. A corporation, business, or other entity formed by or for the benefit of such an individual would be included in the definition, as would immediate family members of such individuals (including spouses, parents, siblings, children and spouses’ parents and siblings), and those who are widely and publicly known (or actually known by the covered financial institution) to be close associates of a senior foreign political figure.

Proceeds of Foreign Corruption

“Proceeds of foreign corruption” includes any asset of a senior foreign political figure acquired by misappropriation, theft, or embezzlement of public funds, the unlawful conversion of a foreign government’s property, or through acts of bribery or extortion, including any other property into which the asset has been transformed or converted.

Filing SARs on Activity that May Involve the Proceeds of Foreign Corruption

A list of transactional red flags that may be indicative of foreign corruption can be found in *Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption*.²⁵ Additional guidance published in 2008, *Guidance*

25. See *Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption* (January 2001), issued by the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the U.S. Department of State, at <http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-9a.pdf>

to *Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption*²⁶ requested that financial institutions include the term “foreign corruption” in the narrative.

FinCEN Guidance

Foreign Corruption Guidance

FinCEN addresses the threat of foreign corruption by promoting more effective reporting by financial institutions of potential illicit activity. Specifically, FinCEN has worked with law enforcement and regulatory partners to provide instructions for financial institutions on the best ways to report possible foreign corruption in SARs, thereby helping law enforcement more easily identify potential corrupt activity. These efforts include the guidance issued by FinCEN in April 2008 regarding the reporting of suspicious activity related to foreign corruption.²⁷ Such guidance helps financial institutions understand how to prevent senior foreign political figures from exploiting potential vulnerabilities in the United States and international financial systems that allow them to disguise or otherwise facilitate illicit activities. Specifically, including the requested term “foreign corruption” in the SAR narrative allows FinCEN and law enforcement to more easily access information related to corruption and monitor for related suspicious activity.

Beneficial Ownership Guidance

On March 5, 2010, FinCEN clarified and consolidated existing regulatory expectations for obtaining beneficial ownership information for certain accounts and customer relationships.²⁸ The guidance indicated that, as part of an effective BSA/AML compliance program, financial institutions should establish and maintain customer due diligence procedures that are reasonably designed to identify, and verify the identity of, beneficial owners of an account based on the institution’s risk determination relative to the account. Obtaining beneficial ownership information may prove especially important in identifying corrupt individuals attempting to mask identity when moving funds moving through the U.S. financial system.

26. See *Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption*, FIN-2008-G005, issued on April 17, 2008, at http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2008-g005.pdf.

27. Ibid.

28. http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-g001.pdf

Advisories on Recent Events in the Middle East

Considering the possible impact of recent events in the Middle East involving Tunisia, Egypt and Libya, FinCEN issued advisories to remind U.S. financial institutions of their requirement to apply enhanced scrutiny for private banking accounts held by or on behalf of senior foreign political figures and to monitor transactions that could potentially represent misappropriated or diverted state assets, proceeds of bribery or other illegal payments, or other public corruption proceeds.²⁹ Identifying and reporting such suspicious transactions or a change in patterns of transactions possibly related to the recent events highlighted is an important component in tracking the movement of funds that may be the proceeds of foreign corruption.

314(a) Process

Section 314(a) of the USA PATRIOT Act, enables Federal, State, local, or foreign law enforcement agencies, through FinCEN, to reach out to more than 45,000 points of contact at more than 25,000 financial institutions to search accounts and transactions of persons that may be involved in terrorist activity or money laundering.

The 314(a) process requires that the requesting agency meet certain requirements, and, if the investigation involves money laundering, the requesting agency must certify that the case is significant. Additionally, the requesting agency must have exhausted traditional methods of investigation. The 314(a) program is intended to support investigations involving terrorist activity or significant money laundering. There may be instances where a request involves a senior foreign political figure who is suspected of laundering the proceeds of foreign corruption.

In these instances, the 314(a) program may prove beneficial in combating foreign corruption. Based upon its proven track record of success in providing new leads to Federal law enforcement, and pursuant to international treaty provisions, FinCEN issued a final rule, in February 2010, expanding the 314(a) program to allow access by international, state, and local law enforcement.³⁰

29. http://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a002.html; http://www.fincen.gov/news_room/rp/advisory/pdf/advis29.pdf; and http://www.fincen.gov/news_room/rp/advisory/pdf/advis18.pdf

30. http://www.fincen.gov/statutes_regs/frn/pdf/20100204.pdf

Financial Action Task Force³¹ (FATF) Participation

The United States has worked with other FATF-member jurisdictions and organizations to develop a paper outlining efforts by FATF to combat corruption. The FATF Corruption Information Note³² was developed to raise public awareness of how the FATF Recommendations, which are the global AML/CFT standards, when effectively implemented, help to combat corruption.³³ FinCEN also provides advisories based on FATF's work related to jurisdictions of money laundering concern.

General Regulatory Requirements Related to Corruption and PEPs

By FinCEN's Office of Outreach Resources

The previous article highlighted and consolidated most of FinCEN's regulations and guidance related to senior foreign political figures. This article discusses general regulatory expectations related to PEPs and corruption. Based on the SARs analyzed in the previous sections of this publication, much of the suspicious activity involving PEPs or corruption appeared to be identified outside the private banking context.

Below we highlight how general due diligence procedures incorporated into a financial institution's anti-money laundering program relate to the suspicious activity connected to PEPs or corruption. The article also responds to commonly asked questions relating to the handling of such accounts.

-
31. "The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. FATF is therefore a "policy-making body" that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. FATF has published 40 + 9 Recommendations in order to meet this objective. See www.fatf-gafi.org.
 32. A Reference Guide and Information Note On the Use of the FATF Recommendations to Support the Fight Against Corruption, at <http://www.fatf-gafi.org/dataoecd/59/44/46252454.pdf>.
 33. FinCEN contributes to the ongoing work of FATF by engaging in discussions with other jurisdictions, regarding senior foreign political figures, proliferation finance, wire transfers, international cooperation, and operational issues relating to FIUs. FinCEN continues to publish advisories to inform banks and other financial institutions operating in the United States of the risks associated with deficiencies in the anti-money laundering and counter-terrorist financing regimes of jurisdictions identified by FATF in its public statements.

Retail Banking

PEP accounts are not limited to large or internationally focused banks. A PEP can open an account at any bank, regardless of its size or location, and may utilize any of its products and services. Accordingly, financial institutions should have risk-based procedures for identifying PEP accounts and assessing the degree of risk involved, which will vary. Risk may also depend on factors such as the purpose of the account, the actual or anticipated activity, products and services used, and size or complexity of the account relationship.³⁵

General Due Diligence

Commensurate with the identified level of risk, due diligence procedures could include, as appropriate, but are not limited to, the following:

- Identifying the accountholder and beneficial owner, including the nominal and beneficial owners of companies, trusts, partnerships, private investment companies, or other legal entities that are accountholders.
- Seeking information directly from the account holder and beneficial owner regarding possible PEP status.
- Identifying the accountholder's and beneficial owner's countr(ies) of residence and analyzing the level of risk for corruption and money laundering associated with these jurisdictions.
- Obtaining information regarding employment, including industry and sector and the level of risk for corruption associated with the industries and sectors, especially if this customer's residency is outside the United States.
- Checking references, as appropriate, to determine whether the account holder and beneficial owner is or has been a PEP.
- Identifying the account holder's and beneficial owner's source of wealth and funds.

34. See FFIEC Manual, at http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf, at 300.

35. See FFIEC Manual, at http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf, at 298.

- Obtaining information on immediate family members or close associates either having transaction authority over the account or benefiting from transactions conducted through the account.
- Determining the purpose of the account and the expected volume and nature of account activity.
- Making reasonable efforts to review public sources of information. These sources will vary depending upon each situation; however, banks should check the accountholder and any beneficial owners of legal entities against reasonably accessible public sources of information (e.g., government databases, major news publications, commercial databases and other databases available on the Internet, as appropriate.³⁶)

If a financial institution determines that a new or existing account is a PEP account, it should evaluate the risks presented by that account, take appropriate steps for opening or maintaining that account, and exercise additional, reasonable due diligence. This may include, but is not limited to, increasing reference inquiries, obtaining additional background information on the PEP from sources in the client's home country, and consulting publicly available information sources.³⁷

Answers to Commonly Asked Questions Related to PEPs and Corruption:

Q: What risks do PEPs present?

Conducting business with PEPs engaged in foreign corruption or other illicit activities could have legal and reputational risks for a financial institution, and could result in heightened regulatory scrutiny and possible supervisory action.

Q: Is there a single officially-sponsored list of global PEPs?

No.

36. See FFIEC Manual, at http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf, at 299.

37. See FFIEC Manual, at http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf, at 300.

Q: What factors should financial institutions consider to determine if an individual is a PEP?

Financial institutions should consider various factors when determining if an individual is a PEP, including: (a) official responsibilities of the individual's office; (b) nature of the office (e.g., honorary or salaried); (c) level of authority or influence over government activities or other officials; and (d) access to significant government assets or funds.³⁸

Q: Are all PEPs high risk?

No. A PEP's geographic location, or position, or the level or nature of influence or authority may affect risk. Likewise, the nature of the PEP's relationship with a financial institution, including the products or services being utilized and the account activity, will also affect risk.

Q: Why is there a greater focus on senior foreign political figures versus senior domestic political figures?

Perception of greater focus on senior foreign political figures may also be attributed to 31 CFR 1010.620, the regulations implementing part of Section 312 of the USA PATRIOT Act. The enhanced due diligence obligation addressed in this part of the regulations is specific to private banking accounts established, maintained, administered, or managed in the United States for senior foreign political figures. Outside of this specific regulatory obligation, the focus a financial institution places on a customer is commensurate with the risk posed by the customer; this may include products and services used, geographic location, and source of funds. If a senior foreign political figure, or any other category of customer, utilizes financial services posing a greater risk of illicit activity, such as cross-border wire transfers or high-frequency debit activity in international jurisdictions, additional scrutiny may be required under general AML program requirements. As part of an account opening procedure or ongoing monitoring activity, financial institutions may identify domestic political figures. As with all products and services offered by a financial institution, those used by domestic political figures must be incorporated into a financial institution's AML program as appropriate. If transaction activity does not coincide with account expectations or stated purpose, with either a domestic or foreign political figure, the financial institution may wish to increase its due diligence.

38. See FFIEC Manual, at http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf.

Q: When are corporations considered senior foreign political figures?

If a corporation, business, or other entity has been formed by or for the benefit of an individual who is a senior foreign political figure, the entity itself could satisfy the definition of a senior foreign political figure.

Q: How should financial institutions monitor PEPs?

Financial institutions should monitor any accounts of PEPs based on the risk they present. Lower-risk customers should be monitored through regular suspicious activity monitoring and customer due diligence processes. Likewise, customers that pose high money laundering or terrorist financing risks present increased exposure to financial institutions – due diligence policies, procedures, and processes should be increased as a result. High-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the financial institution.

Q: What should financial institutions do if a PEP’s status changes?

As with any change in a customer’s risk profile (e.g., expected account activity, change in occupation or business operations), the customer’s risk rating should be re-assessed based on established policies and procedures for maintaining or changing customer risk ratings. If appropriate, heightened due diligence should be conducted on the account.

Q: Why does my screening process return a “PEP” hit, and what do I do when it returns a hit?

FinCEN understands that many vendors of screening products will concurrently screen against OFAC’s Specially Designated Nationals list³⁹ and other lists they offer as a service to their clients. Such additional lists may include the Central Intelligence Agency’s directory of Chiefs of State and Cabinet Members of Foreign Governments,⁴⁰ a proprietary list maintained by the vendor, or lists maintained by other U.S. government or foreign government agencies. The vendor software may label a match found in one of these external lists a “PEP.” FinCEN does not maintain or endorse any list of politically exposed persons, and FinCEN’s Regulatory Helpline is unable to verify whether a customer is the same as an

39. For more information about OFAC’s Specially Designated National s list, see <http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx>.

40. See <https://www.cia.gov/library/publications/world-leaders-1/index.html>.

individual identified in any externally maintained “PEP” lists. However, searching commercial and other publicly available lists is one among several possible methods for identifying or verifying that a customer may be a politically exposed person. Armed with a full understanding of its vendor’s unique screening processes, a financial institution could consider how these might fit into its risk-based approach for identifying PEPs.

Q: If a financial institution files a SAR on a PEP, should the financial institution end the customer relationship?

The decision to terminate a customer relationship is a business decision. There is no requirement under the Bank Secrecy Act to terminate a customer relationship based solely on the filing of a SAR.

A View from Miami

By A Supervisory Special Agent of Immigration and Customs Enforcement

The South Florida Miami SAR Review Team is comprised of representatives from the US Attorney’s Office along with ICE, Homeland Security Investigations, IRS, FBI, DEA, Department of State, Diplomatic Security, US Secret Service, Department of Labor, FDIC and the Federal Reserve. On a monthly basis, the team meets to review a select number of SARs submitted by financial institutions during the previous thirty days. For a large metropolitan area like Miami, we narrow down the search parameters to review only SARs that meet certain variables and fall in certain targeted zip codes. This allows the team to look at a manageable amount of SARs in a productive manner. Prior to the monthly meetings, the SARs are assigned evenly to each of the agencies that attend. Each agency representative analyzes their assigned SARs in advance of the meeting. At the meeting, the content of the SARs are discussed to determine the possible underlying criminal activity and decide which agency will take further investigative action, if needed.

South Florida has always been a favorite destination for international visitors and political figures, whether it is for vacation or to purchase property along its sandy and sunny beaches. As such, Miami finds itself in the distinct position of being a reoccurring hot spot for funds pilfered by politically exposed persons (PEPs) and other criminal proceeds. This fact resulted in the establishment of the Foreign Public

Corruption Task Force by the US Customs Service in 2003. This first of its kind task force focuses solely on the identification and seizure of assets related to PEPs and the criminal prosecution of any US violators connected to the laundering of the proceeds of foreign public corruption. This task force carried over to ICE, Homeland Security Investigations and, today, is a national leader in these types of investigations.

With the environment such as it is in Florida and its attractive draw to foreigners seeking to place their funds in a warm, sunny and safe place, the Miami SAR Review Team, as well as my fellow agents at Homeland Security Investigations, take particular notice of the type of funds that are finding their way into our financial infrastructure. We regularly encounter PEP type cases emerging from the SAR reviews, as well as from leads received from foreign governments and during the course of our regular investigative activities. During an average SAR Review, limiting the quantity as described above, the team will review in excess of 100 SARs each month. Of those reviewed, we regularly see between 1 and 3 SARs that are determined to be PEP related. There are some commonalities in these SAR filings that are of note.

The majority of the SARs filed that are determined to be PEP related do not actually spell out “politically exposed person,” “PEP,” “corruption” or “bribery” as key phrases. Instead, the determination is made by the team based upon various identifiers in either the subject section or the narrative description. It is more likely the case that the team makes the identification by noting that the suspect’s occupation is listed as an occupation that would move the suspect into the category of PEP, such as “general in army” or “consulate official.” In instances where this type of occupation is not listed or no occupation is listed at all, the determination that the SAR is PEP related is often made based upon the totality of the facts outlined in the SAR. For instance, the SAR may detail that the listed subject has a relative that is a high ranking government official and some of the transfers appear to come from that relative or that the beneficial owner of the account may have held a high level office or that the transfers conducted appear to be related to a government contract. In many instances, the identification that the SAR should be approached as a potential PEP case comes after review and consideration, rather than from direct identification by the financial institution. Further, it is the rare circumstance when the bribery box is checked on a PEP SAR, even when there is a potential for bribery to have occurred. This is likely due to the level of proof that the preparer would like to have before making a judgment that the subject has taken direct bribes. The transactions outlined in most SARs, although suspicious, could be evidence of a number of different possible criminal acts, thus making the determination that it is specifically

bribery difficult. Despite this, the SARs that link to PEPs are being identified and investigated; however, any key word search for terms like PEP, public corruption or bribery would likely omit numerous potential cases.

In the majority of the PEP SARs, the narrative's concentration is on the potential criminality demonstrated by the financial transactions, rather than the status of the violator, as is reasonable. In most instances, the SAR will detail activity that resembles a fraud or a money laundering scheme with some reoccurring red flag indicators. Large deposits, frequent wire activity or financial transactions that would largely exceed the salary of a public official is one of these patterns, especially evident where the PEP is identified as a controlling party to the account. The use of shell entities in an attempt to mask the beneficial ownership of the account when the account is connected to a public official or the payment of a government contract would also raise suspicion. The rapid transfer of funds between seemingly unrelated accounts or the layering of funds between accounts controlled by the same individuals should also be considered a red flag. All of these types of behaviors, however, could also be indicative of other types of criminal activity. They often result in the conclusion that the account is being utilized as a conduit for fraud or some unspecified money laundering, without highlighting the connection to the PEP.

It would be helpful to law enforcement and to SAR Review Teams in general if financial institutions, when preparing their SARs try to identify any potential PEP early in the SAR.⁴¹ This would be helpful even if the PEP is only tangentially connected to the activity of the account. Any potential PEP connection is useful information to an investigator. It is imperative that the preparer clearly identify each account controller and the relationship to the accounts identified. The designation of an account holder as a PEP can easily be accomplished in the occupation box of the subject section of the SAR or by merely using the key word "PEP" or "politically exposed person" in the beginning of the narrative. The first few lines in the narrative are critical for law enforcement, as they help to set the tone for what the overall suspicious activity and nature of the potential violations would be in the SAR. SAR preparers should always make a summary statement of their observed suspicious activity in the first few lines of any SAR. This helps SAR Review Teams to understand what they are looking for in a SAR early in the review process, properly identify where the SAR would best be assigned and assists any investigating agency to utilize key word searches to find SARs relating to a specific area of concern.

41. FinCEN guidance dated April 17, 2008 also instructs filers to use the key term "foreign corruption."

SARs have been an indispensable tool for law enforcement, both in initiating investigations and in contributing to ongoing cases. ICE Homeland Security Investigations has had several significant successful investigations that were initiated through SARs. In the PEPs area, we are counting on the continued vigilance of the financial community in identifying suspicious accounts and reporting those activities to assist law enforcement in their efforts to safeguard our financial infrastructure.

**Priorities and Initiatives of the Asset
Forfeiture and Money Laundering Section
(AFMLS), United States Department of Justice**
By Jennifer Shasky Calvery, AFMLS Chief

Criminal organizations are businesses. Like any business, profit is their primary motivation. These organizations - whether they be a violent drug cartel operating along our Southwest Border, an Eastern European cyber-criminal organization targeting our populace over the Internet, or a Chinese criminal organization pirating and manufacturing unsafe consumer goods for distribution in the United States, exploit the fullest range of criminal activity to make money and use their assets to expand their influence and their capital. To stop these criminal enterprises, we must destroy their financial infrastructures and prevent them from exploiting vulnerabilities within our financial systems. The U.S. Department of Justice aims to do just that through aggressive use of our asset forfeiture and anti-money laundering laws. When the Department forfeits criminal proceeds and vigorously prosecutes money laundering violations, we can shut down criminal businesses and frustrate their ability to operate in this country.

But the Department cannot fulfill this mission alone. We look to financial institutions to serve as the first line of defense against illegal money entering the system. SARs filed by financial institutions provide invaluable information to law enforcement by revealing illegal activity that might otherwise have gone undetected. Over the years, SARs have become the building blocks of countless prosecutions and civil forfeiture cases across the country.

AFMLS Priorities and Initiatives

This article will highlight two of AFMLS' top priorities in the money laundering arena - targeting gatekeepers and promoting transparency - and how we are pursuing those priorities. Specifically, these priorities focus on the pursuit of those who facilitate money laundering and the promotion of greater transparency in the financial industry. At the same time, our initiatives seek to aggressively use the asset forfeiture and money laundering laws to attack the financial tools exploited by official foreign corruption and to dismantle the infrastructure of the Mexican drug cartels and other international organized crime syndicates.

Going after Facilitators

Gatekeepers, or what I will refer to as facilitators, leverage their standing and credibility as industry professionals to facilitate and promote illegal financial activity. These corrupt professionals, such as lawyers, accountants, and bankers, use their status to enable criminal behavior by circumventing compliance regimes designed to prevent the introduction of illicit funds into the U.S. financial system. Following the money is often the best, and sometimes the only, way for law enforcement to track and ultimately disrupt criminal conduct. By disguising the source of dirty money, facilitators not only imperil investigations of past crimes, but provide the means for the commission of future ones. Identifying and prosecuting these facilitators, particularly those who assist kleptocrats, drug cartels, and other international organized crime groups to evade anti-money laundering safeguards, is a top priority of AFMLS.

Transparency

A second AFMLS priority is promoting transparency within the financial industry and combating the use of shell companies to conceal criminal activity. Both foreign and domestic law enforcement face considerable difficulties when investigating U.S. shell corporations due to the lack of beneficial ownership information available in the United States.

In the vast majority of cases, investigations involving suspicious activity conducted through a U.S. shell company invariably lead to a dead end – and therefore are simply dropped. Internationally, lack of beneficial ownership information can also hamper our ability to respond to requests for assistance from our foreign counterparts. This problem not only damages our reputation, but also undermines our efforts to join with foreign counterparts in a global offensive against organized crime and terrorism.

Because the United States regularly encourages its international partners to implement robust AML regimes, it is critical that we lead by example to close any gaps in our own system. Corporate transparency is just such a gap. AMFLS is therefore working with our Treasury colleagues and Congress to craft appropriately tailored legislation that will enable us to identify the living, breathing beneficial owner of a legal entity in the United States at its incorporation. We also support the U.S. Department of the Treasury and Financial Action Task Force efforts to encourage greater due diligence in this area by financial institutions. We, in law enforcement, are definitely cognizant of this issue as our investigations consistently indicate the importance of beneficial ownership information in pursuing money laundering and asset forfeiture cases that implicate financial institutions operating in the United States.

Kleptocracy Asset Recovery Initiative

The Department of Justice's Kleptocracy Asset Recovery Initiative is designed to target and recover the proceeds of foreign official corruption that find their way into our banking and financial systems. Once fully implemented, the Department will pursue civil forfeiture cases to recover assets derived from high-level foreign corruption. The timeliness and need for this initiative is underscored daily by events around the world, as we witness both Egypt and Tunisia reportedly launch their own corruption investigations in the wake of regime changes. It is clear that in many countries there is popular frustration with the corruption and the looting of state assets that leave the populace short-changed.

But our efforts can only accomplish so much; denying kleptocrats access to the U.S. financial system in the first place is an even more important goal. And, like asset recovery, this requires cooperation between financial institutions and law enforcement. Financial institutions can deny kleptocrats access to their institutions by refusing to do business with them. At a minimum, they are required to identify and report when financial professionals are facilitating kleptocrats' activities, both through the use of their professional capacity and through shell companies. Together, we can prevent these facilitators from using the United States as a safe haven for kleptocrats who attempt to treat state assets as their own. And when we do not achieve prevention, together we can work to recover corruption proceeds to be returned for the benefit of the people in the victim countries.

Writing Effective SAR Narratives

By FinCEN's Office of Outreach Resources

In April 2008, FinCEN published guidance⁴² to assist financial institutions in filing SARs on activity related to foreign corruption. In the guidance, financial institutions were instructed to include the term “foreign corruption” in the narrative portion of the SAR.

Analysis of SAR filings reporting foreign corruption included a review of SAR narratives to ascertain the details of the activity being reported. In addition to the analytical findings reported in this issue, this analysis provides FinCEN with an opportunity to offer feedback to filers on the quality of SAR narratives.

The Importance of the SAR Narrative

SAR narratives play an important role in understanding potential illegal activities, and assist law enforcement in detecting and preventing the flow of illicit funds. In addition to the value that SAR filings bring to law enforcement, and to regulatory agencies in conducting their work, FinCEN utilizes BSA data in our analytical products, which can provide important information to law enforcement, regulatory agencies, and the financial industry.

SAR narratives have helped in determining the breadth of mortgage fraud activity, identity theft and trade based money laundering, just to name a few. For all the foregoing reasons, it is critical that the information conveyed in SAR filings be as accurate and complete as possible. The narrative section should identify the essential elements of the suspicious activity being reported – *who, what, where, when* and *why* – and should be a complete account of the activity and follow a chronological order.

To assist filers in providing more effective SAR narratives, we remind filers of these key elements and highlight ways to improve the narrative portion of a SAR, specifically by use of examples from the analysis done for this issue:

42. http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2008-g005.pdf

Who is conducting the activity?

- In the narrative, describe the known information about the suspect(s) reported in the appropriate section of the form including, for example, with respect to a senior foreign political figure, title, occupation, or nature of the suspect's business.
- If more than one individual or business is involved in the suspicious activity, identify all suspects and any known relationships among them to the fullest extent possible.
- If a senior foreign political figure is detected as a beneficial owner of a company, provide information on the business.
- A senior foreign political figure may use family members and close associates to facilitate hiding the corruption proceeds. Likewise, suspicious activity may also be conducted through the use of intermediaries, such as an attorney or accountant. If any such relationships are identified, they should be included in the narrative.
- Note whether the senior foreign political figure is the institution's customer/ account holder or another party to the transaction, such as an originator of a wire.

What instruments or mechanisms are being used in the transaction(s)?

- An illustrative list of instruments or mechanisms that could be used in suspicious activity involving corruption includes, but is not limited to, private banking, wire transfers, bank drafts, use of shell companies, or the use of correspondent accounts or escrow accounts.
- If a shell or operational company is being used, note whether the senior foreign political figure is a beneficial owner.
- It may prove useful to note whether the senior foreign political figure is utilizing retail banking services or more generally the type of account utilized.
- Identify all accounts involved in the suspicious activity, including those of known relationships that the filer believes may also be involved.

Where did the suspicious activity take place?

- Identify the jurisdictions where the accounts and subjects are located.

When did the suspicious activity take place?

- If a pattern of activity has been occurring over a period of time, state when the suspicious activity was first noticed, the duration of the activity and whether the activity has changed over time.
- Also, note if a previous SAR was filed.

Why does the filer think the activity is suspicious?

- Describe as fully as possible why the activity or transaction is unusual for that customer. For example, if a family member of a senior foreign political figure is sending or receiving large dollar wire transfers for which there is no apparent reason or which do not correspond with the customer's profile, this may be an indication that the account is being used to move or hide the proceeds of corruption.

Example of an Effective Narrative

BANK A (THE BANK) CONDUCTED A REVIEW OF AN ACCOUNT HELD BY THERESA SMYTHE (SMYTHE), WIFE OF PRESIDENT EDWARD SMYTHE, A POLITICALLY EXPOSED PERSON, ACCOUNT #12345678. A PRIOR SAR REPORTED SUSPICIOUS INCOMING WIRES INTO SMYTHE'S ACCOUNT AND POSSIBLE STRUCTURING. THIS ACTIVITY IS ONGOING, AND THE REVIEW IDENTIFIED SUSPICIOUS ACTIVITY IN A NEW ACCOUNT HELD BY THERESA AND A JOINT ACCOUNT HOLDER, BRYAN JONES (JONES), WHO HAS BEEN IDENTIFIED IN NEWS REPORTS AS THERESA'S SON. PUBLICLY AVAILABLE INFORMATION HAS PRESIDENT EDWARD SMYTHE AND WIFE THERESA (COLLECTIVELY, "THE SMYTHES"), AS BEING INVOLVED IN CORRUPTION AND THAT PROCEEDS OF THE CORRUPTION HAVE BEEN FUNNELED THROUGH SHELL CORPORATIONS AND FAMILY MEMBERS TO BENEFIT THE PERSONAL INTERESTS OF THE SMYTHE FAMILY. THE BANK NOTED SUSPICIOUS ACTIVITY IN THE JOINT ACCOUNT OF SMYTHE AND JONES, ACCOUNT #34567890 (OPENED IN SEPTEMBER 2010.) A TRANSACTION REVIEW OF ACCOUNT #34567890 REVEALED THAT BETWEEN SEPTEMBER, 2010, AND DECEMBER, 2010, THERE WERE \$480,000 IN INCOMING WIRES FROM AN ACCOUNT IN LONDON, UK AND \$205,000 IN OUTGOING CASH TRANSACTIONS AND CHECK CARD PURCHASES, INCLUDING TO LUXURY RETAILERS. ON 10/5/10, A WIRE FOR \$130,000 WAS DEPOSITED TO ACCOUNT #234567891 AT BANK B AND REFERENCED THE PURCHASE OF A LUXURY AUTOMOBILE. SMYTHE CONDUCTED A CASH WITHDRAWAL FOR \$8,000 ON 10/15/10, \$6,500 ON 10/17/10, \$7400 ON 10/31/10, AND \$9,200 ON 11/2/10. ON 11/22/10, JONES PURCHASED A CASHIER'S CHECK FOR \$32,000 MADE PAYABLE TO HIMSELF, WHICH WAS DEPOSITED INTO AN ACCOUNT HELD AT BANK C. ON THE SAME DAY, HE ALSO INITIATED A TRANSFER OF \$60,000 TO THOMAS JONES, WHICH WAS DEPOSITED TO PERSONAL CHECKING ACCOUNT #345789234 HELD AT BANK A. THE WIRE REFERENCED "PERSONAL TRANSFER". THE BANK CONSIDERS THE EXCESSIVE INCOMING WIRE AMOUNTS, PAYMENTS FOR LUXURY GOODS AND OTHER WITHDRAWALS TO INDICATE POSSIBLE STRUCTURING AND POTENTIAL ATTEMPTS TO HIDE FOREIGN CORRUPTION PROCEEDS.

Why this narrative is effective:

This narrative contains all of the key elements of an effective narrative: *who* is conducting the activity, including associated relationships the filer has identified, *what* instruments are being used (wires and cashier's checks), *where* activity occurred, *when* the transactions took place, and *why* the filer believed the activity was suspicious (news reports discussing potential corruption, large incoming wire amounts, potential structuring, etc.)

Example of a Less Effective Narrative

BANK A (THE BANK) CONDUCTED A REVIEW OF AN ACCOUNT HELD BY THERESA SMYTHE (SMYTHE) WHO IS THE WIFE OF A POLITICALLY EXPOSED PERSON. A PRIOR SAR REPORTED SUSPICIOUS INCOMING WIRES INTO SMYTHE'S ACCOUNT AND POSSIBLE STRUCTURING. THIS ACTIVITY IS ONGOING, AND THE REVIEW IDENTIFIED SUSPICIOUS ACTIVITY IN A NEW ACCOUNT HELD BY THERESA AND A JOINT ACCOUNT HOLDER WHO HAS BEEN IDENTIFIED AS THERESA'S SON. PUBLICLY AVAILABLE INFORMATION HAS THERESA AND HER HUSBAND HAVE BEEN INVOLVED CORRUPTION AND THAT PROCEEDS OF THE CORRUPTION HAVE BEEN FUNNELED THROUGH SHELL CORPORATIONS AND FAMILY MEMBERS TO BENEFIT THE PERSONAL INTERESTS OF THE SMYTHE FAMILY. THE BANK NOTED SUSPICIOUS ACTIVITY IN THE JOINT ACCOUNT OF SMYTHE AND HER SON (OPENED IN SEPTEMBER 2010.) A TRANSACTION REVIEW OF THE ACCOUNT REVEALED THAT BETWEEN SEPTEMBER, 2010, AND DECEMBER, 2010, THERE WERE NUMEROUS INCOMING WIRES FROM AN ACCOUNT IN LONDON, UK AND OUTGOING CASH TRANSACTIONS AND CHECK CARD PURCHASES, INCLUDING TO LUXURY RETAILERS. ON 10/5/10, A WIRE WAS DEPOSITED TO AN ACCOUNT AT BANK B AND REFERENCED THE PURCHASE OF A LUXURY AUTOMOBILE. SMYTHE ALSO CONDUCTED CASH WITHDRAWALS ON 10/15/10, 10/17/10, 10/31/10, AND 11/2/10. ON 11/22/10, SHE PURCHASED A CASHIER'S CHECK MADE PAYABLE TO HERSELF, WHICH WAS DEPOSITED INTO AN ACCOUNT HELD AT BANK C. ON THE SAME DAY, SHE ALSO INITIATED A TRANSFER TO THOMAS JONES, WHICH WAS DEPOSITED TO A PERSONAL CHECKING ACCOUNT HELD AT BANK A. THE WIRE REFERENCED "PERSONAL TRANSFER". ACCORDING TO THE BANK'S RECORDS, THERESA DOES NOT APPEAR TO BE EMPLOYED AND THERE IS NO EXPLANATION FOR THE SOURCE OF FUNDS GOING IN AND OUT OF THE ACCOUNT, ADDITIONALLY, THE BANK CONSIDERS THE EXCESSIVE INCOMING WIRE AMOUNTS, PAYMENTS FOR LUXURY GOODS AND OTHER WITHDRAWALS TO INDICATE POSSIBLE STRUCTURING AND POTENTIAL ATTEMPTS TO HIDE FOREIGN CORRUPTION PROCEEDS.

Why this narrative is less effective:

The narrative does not describe any specific account information (account numbers, type of account, or names of other account holders), nor does it specifically name the PEP with a connection to this account. It also does not contain critical transactional information, such as dollar amounts, that alerted the filer to potential suspicious activity. As a result, it is of less value to law enforcement as part of an investigation than a narrative that does include such details. Providing even such information as account numbers, names associated with the accounts or types of products or services utilized by the customer can help inform law enforcement as part of an investigation even if no specific activity was identified as suspicious.

Additional information is available to filers in preparing suspicious activity reports. In November 2003, FinCEN published SAR Narratives Guidance⁴³ that provides further assistance to filers in completing effective SAR narratives. In Issue 16 of *The SAR Activity Review – Trends, Tips & Issues*, representatives from law enforcement agencies provided suggestions on preparing suspicious activity reports.⁴⁴ In the same issue, FinCEN provided information to filers on avoiding common SAR errors.⁴⁵ Questions on how to complete SARs may also be directed to FinCEN's Regulatory Help Line at 800-949-2732.

43. http://www.fincen.gov/statutes_regs/guidance/pdf/narrativeguidance_webintro.pdf.

44. See *The SAR Activity Review – Trends, Tips and Issues* (Issue 16, October 2009), page 45, Law Enforcement Suggestions When Preparing Suspicious Activity Reports.

45. See *id.*, page 48, Avoiding Common Errors in Suspicious Activity Reports.

Section 5 – Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into an aspect of compliance management or fraud prevention. The *Industry Forum* section provides an opportunity for the industry to share its views. The information provided may not represent the official position of the U.S. Government.

For this issue, FinCEN invited three financial institutions of varying asset sizes and business profiles to share their perspective on the challenges in identifying customers who are politically exposed persons, and maintaining accounts for such persons. Through conversations within the Bank Secrecy Act Advisory Group, institutions of various sizes, product types, geographic location, and customer bases identified differing ways of identifying PEPs and challenges associated with monitoring for such activity. However, throughout these articles, readers will also note that even though there may be differences among these institutions in how they handle such accounts, they approach the topic with similarities as well. We encourage readers to consider the challenges they may face regarding this issue and how the perspectives of these institutions, and the points they raise in each article, can help inform their own AML/BSA compliance programs.

Challenges & Limitations of Identifying PEPs & Determining Relevant Risks

By Marta Perez-Pendas, Esq., Pacific National Bank

Representing Florida International Bankers Association, Bank Secrecy Act Advisory Group

There is little argument that banking relationships with Politically Exposed Persons – PEPs – create increased risks for financial institutions. PEPs are by no means money launderers or embezzlers merely because of their PEP designation. The positions they hold, however, create greater opportunity for misuse of power

and influence and thereby pose an increased reputational and regulatory risk. Financial institutions must devise the means for identifying and controlling the risks associated with PEPs, but the task is not an easy one.

The PEP definition, perhaps by necessity, is both subjective and broad. The FFIEC defines PEPs to include current or former senior foreign political figures, their family and close associates. The term “political figures” is fairly easy to define (i.e., elected or appointed officials of foreign governments or foreign political parties and executives of foreign government-owned corporations – and entities formed by or for their benefit). It is not easy, however, to determine what makes someone a senior political figure (an SPF). There are no rules for applying the “senior” qualifier – making the determination largely subjective. Do the same rules of “seniority” apply for all countries? When does a “middle-ranking” position - in any given foreign country - become a “senior” position? An exact application of this qualifier might require considerable knowledge of the political infrastructure of each PEP customer’s country of origin – as well as specific rules applicable for each country.

Beyond subjectivity, the broad nature of the definition, and in particular the “family and close associates” spokes on the PEP definition wheel, raises additional issues. Family includes parents, siblings, spouse, children and in-laws – but are there instances where other family members pose a PEP risk? When are these other family members close enough to warrant concern? Can family members include U.S. citizens and/or residents? The inclusion of “close associates” poses similar problems. “Close associates” are generally limited to “widely and publicly known” contacts with the authority to conduct financial transactions on behalf of a PEP. In reality, however, most close associates with such level of authority are not widely or publicly known – and they are difficult, if not impossible, to identify.

An ever increasing PEP population generates additional difficulty. The phrase “once a PEP, always a PEP” is well-known in compliance circles. The concept may have a sound basis (the fruits of misuse of power do not necessarily surface solely during the active political term of a PEP), yet it is cumbersome to apply a PEP designation ad infinitum. In addition, non-PEP customers can become PEPs, sometimes without a financial institution’s knowledge. A public event, such as an election covered by media, may be detectable, but other triggering events, such as marriages to PEP family members or promotions from “middle” to “senior” positions – may not be.

To enhance their ability to identify PEPs, financial institutions typically enlist the aid of global PEP databases offered by commercial providers. However, those providers face the same types of difficulties in identifying PEPs and, in the end, their databases will contain only the names of individuals identified by the provider.

Having a foreign country presence or ties, especially those with foreign affiliates, may also provide a significant resource for identifying and risk rating PEPs. In-country bankers are privy to a wider base of knowledge regarding PEPs from their country, and U.S. financial institutions can leverage foreign affiliate knowledge (even when cumulative privacy laws may impede information sharing to a degree).

Identifying PEPs is merely a first step. A second one is defining the level of risk each PEP poses. Not all PEPs present equal risk. PEPs from countries where corruption is widespread carry an ultra-high level of risk, while PEPs from other less volatile countries pose a lesser risk. The difficulty here is that foreign political environments are subject to rapid change – and a PEP that poses minimal risks today, can easily become a high-risk PEP as a result of changing events in the PEP's foreign home country.

Moreover, positions held by PEPs can carry varying degrees of opportunity for misuse of power, and should thereby carry varying degrees of risk. Identification of a customer's status as a PEP should not necessarily result in categorization of the customer at a defined High-Risk level. Financial institutions with a significant PEP population may wish to consider developing a specific set of risk-rating criteria for that will generate stratified levels of PEP risks, in essence, a risk rating within risk rating.

In sum, there are no simple solutions to managing PEP risk, but there are choices. A subjective and broad definition and flexible procedures that apply subjective and comprehensive criteria to a broad customer knowledge base under a holistic approach will likely yield more effective results than an application of an inflexible set of defined rules. A periodic screening of the entire customers base, including signers and holders of powers of attorney (as well as majority shareholders, senior officers and directors, in the case of corporate accounts), against available PEP databases is an essential step. Similarly, regular reviews of identified PEPs should be conducted to verify or, where appropriate, to modify PEP risk levels; and in those situations involving significant PEP customer populations, the stratification of PEP risks may be required.

Who is a Politically Exposed Person: Challenges in Identifying PEPs

*By Kevin Anderson, Director and Michelle Neufeld, Director
Representing Bank of America on the Bank Secrecy Act Advisory
Group*

The global community is greatly impacted by the effects of political corruption. One needs look no further than Riggs Bank, once one of the oldest banks in the country, which now no longer exists, in large part due to the reputational damage suffered from banking several allegedly corrupt foreign leaders. However, there are a number of significant challenges with identifying Politically Exposed Persons (“PEPs”) in general, let alone corruption. This article focuses on some of the issues faced by large commercial financial institutions as they attempt to identify Politically Exposed Persons in their customer base.

The World Bank, as part of its Stolen Asset Recovery Initiative (“StAR Initiative”), indicated that:

over the past 25 years, the whole world has learned about the gross abuses of corrupt ‘politically exposed persons’ (“PEPs”), and through outrageous examples, the way in which they plunder state assets, extort and accept bribes, and use domestic and international financial systems to launder their stolen assets. We do not know the amount of public assets stolen or extorted by prominent office holders – referred to as grand corruption – and mostly laundered through financial institutions, in particular, through banks. The proceeds of corruption stolen from developing countries alone ranges from \$20 billion to \$40 billion per year – roughly equivalent to the annual GDP of the world’s 12 poorest countries where more than 240 million people live.⁴⁶

With this as a backdrop, we’ve outlined some questions that financial institutions should consider in evaluating the risks involved with providing financial services to PEPs and suggest that a continuing dialogue between the public and private sector increases our mutual likelihood of success in reducing corruption.

46. World Bank, “Politically Exposed Persons: Preventative Measures for the Banking Sector,” (May 11, 2010) p. xiii.

PEPs, or as defined within U.S. law, Senior Foreign Political Figures, refer to the following⁴⁷:

- i. A current or former:
 - a. Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not)
 - b. Senior official of a major foreign political party
 - c. Senior executive of a foreign government-owned commercial enterprise
- ii. A corporation, business or other entity that has been formed by, or for the benefit of, any such individual
- iii. An immediate family member of any such individual (Immediate family member means spouses, parents, siblings, children and a spouse's parents and siblings)
- iv. A person who is widely and publicly known (or is actually known by the relevant covered financial institution) to be a close associate of such individual

Within the definition of senior foreign political figure, the first question that arises is what is meant by "senior." While the regulations indicate that "a senior official or executive means an individual with substantial authority over policy, operations, or the use of government-owned resources," this still leaves significant room for interpretation. While some positions are clearly senior, such as the head of state, members of the national legislative and judicial branches, it gets trickier to determine as one moves further down the hierarchical order. For example, are the equivalents of state governors, legislators and judges considered senior? If so, does one continue down to county or municipal level? What if the city is a major one, such as London, Vancouver, Rio de Janeiro or Beijing; do these merit inclusion? Within the military ranks, as an example, the United States Army, Marines and Air Force can have approximately 19 four-star generals, but up to 498 active-duty generals at one point in time. The further down the hierarchical order one goes, the list of "senior" officials expands significantly.

47. 31 CFR 1010.605(p)

The list explodes when one starts to consider the close known associates and family members of the senior foreign political figures. What may appear to be simple, such as determining the family members, can pose a challenge. In some instances, such as in the UK, where the members of the royal family are well documented, this is relatively easy. However, this is not always the case; for example, press reports on – and well publicized asset freeze orders against – Libyan leader Muammar Gadhafi list between four and ten children. Even more complicated are the close known associates, as these are usually identified through press reports, many of which may need to be assessed for their independence, accuracy and whether they are trying to push a particular agenda. The definition of “close” associate is also further clouded due to the lack of clarity in the definition; for example, would this include a joint business owner and if so, is there a standard threshold for making this determination? Does it include former business owners? Does it include the fellow board members of a company when a former politician is brought on the board? Is it triggered by merely appearing together in a photograph?

Many financial institutions turn to third party vendors who have developed PEP lists and scanning solutions for the financial community since it is impracticable to employ their own limited resources to create and maintain a list themselves. However, this reliance is not without risk, as the Senate Permanent Subcommittee on Investigations indicated “some vendors relied on by U.S. financial institutions to screen clients for PEPs used incomplete and unreliable PEP lists,⁴⁸” noting that several institutions did not identify PEPs as its vendor did not detect family members or close associates. One of the concerns with the PEP lists is not having sufficient additional identifying information on the persons in the lists to enable financial institutions to resolve a potential match. Often, a lack of ability to resolve a potential match on a name alone will force an institution to make a decision as to whether to treat a potential PEP as a true PEP or whether to consider the lack of positive identification as indicating the customer is not a PEP. This becomes extremely critical when dealing with large volumes; a 10 percent match rate when looking at 10 million names results in 1 million items to review.

48. *Keeping Foreign Corruption out of the United States; Four Case Histories; Majority and Minority Staff Report* U.S. Senate Permanent Subcommittee on Investigations, February 10, 2010, p. 6.

The PSI report indicated that to resolve this issue, it would be beneficial for financial institutions to be required to use reliable PEP databases to screen clients. This presents challenges, such as how is one to determine what is a reliable list. Will the government (e.g., regulators) need to certify databases? Would it be more efficient and more effective for government to provide a listing of those persons or jurisdictions it considers to be a higher risk? While there are political considerations that would complicate the compilation of such a list, there is a precedent for listing certain countries as posing heightened money laundering concerns, such as the Department of State's annual International Narcotics Control Strategy Report ("INCSR"), and countries deemed to represent a heightened risk of corruption, such as the efforts by the World Bank, the International Monetary Fund ("IMF"), Transparency International's Corruption Perceptions Index and the U.S. Department of State's reporting under the International Anticorruption and Good Governance Act.

With all the focus on senior "foreign" political figures, it leaves open the question of whether PEPs should include domestic persons as well. The Financial Action Task Force ("FATF") recently issued a consultation paper that recommended including domestic PEPs into the scope of what financial institutions should consider. While acknowledging that domestic PEPs are generally lower risk, and should thus be subject to lesser levels of due diligence, FATF's proposal would further expand the list of PEPs that financial institutions need to consider. This would have a particularly interesting impact when considering the nature of the financial institution that is banking the PEP. A small community bank might consider the town mayor to be a PEP, while a large national bank likely would not.

In addition and in the absence of specific guidelines, institutions should carefully consider how long they should consider a PEP a PEP. In the UK, general guidance is for a year after the removal from the position. To effectively assess this would require an institution to develop a process to identify when PEPs are removed from office and to apply this information to their customer portfolios, including the customers who are not politicians themselves, but are close associates or companies identified as being established by or for the benefit of the PEP. In some cases, it may be easier – and certainly more conservative - to simply indicate that once a PEP, always a PEP, as this removes this cumbersome step and removes opportunities to second guess a decision to lower the customer's risk rating. However, institutions should weigh this approach against the amount of due diligence it requires on an ongoing basis for such customers and assess the best approach to risk management.

Once the financial institution has identified a customer as a PEP, it must then determine the risk that customer poses to it. There is a common assumption that all PEPs are high risk. The risk-based approach dictates that risk posed by a customer will fall along a spectrum of risk some being lower and others being higher. If this is true then logically the same must hold true for PEPs. If we look at the US regulations we see that PEPs appear only in Section 312 of the USA PATRIOT Act where we are told that PEPs with private bank accounts should be subject to higher scrutiny and “enhanced due diligence.” Following the logical argument then, PEPs who have something less than a private bank account could be afforded a lower risk rating.

The Federal Financial Institutions Examination Council (“FFIEC”) indicates that “banks should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior political figures, their families and their associates.⁴⁹” It also recommends banks take a risk-based approach and provides risk factors and mitigation steps to address the risks posed by PEPs. This statement supports the logic outlined above. For example, would a credit card be considered higher risk if it was offered to a PEP; would it make a difference if it was a card with a \$500 limit and was issued to a student at a local college, who is a PEP by virtue of being the son or daughter of a politician? If the institution considers this to be a lower risk customer, how will they be able to determine – and at what point should they determine – that the relationship becomes a higher risk – when the customer graduates and gets a higher limit on the card, when the customer expands the relationship to obtain additional services, such as a checking account (and does it matter whether the child is still a student)? These are all practical considerations that institutions should evaluate when dealing with PEPs. Some will take a more conservative approach and treat all PEPs as higher risk, regardless of the nature of the relationship while others likely will take a more detailed and refined approach. However, institutions will not always be treating these relationships consistently. This is one of the results of the risk-based approach; it will not always lead to consistent results.

One final significant challenge with PEP identification is determining whether an account is established by or for the benefit of a PEP when the PEP’s name is not clearly identified during the establishment of the customer relationship. This

49. FFIEC, “BSA/AML Examination Manual,” (April 29, 2010) p. 297.

typically happens when a legal entity, such as a corporation, partnership or trust, is formed where the PEP's involvement is not disclosed. As the global financial community gets better at identifying these individual relationships, in order to successfully launder the proceeds of corruption will require a certain sophistication that may involve using third parties or creating legal structures that have not yet been linked to the PEP and therefore will not be identified as such through the commercial scanning solutions. Further, financial institutions are subject to varying levels of requirements when it comes to identifying beneficial owners of accounts or customers. When financial institutions undertake efforts to identify the ownership of entity customers, often, the information is only as good as the information the customer provides, as there may not be independent sources that an institution can use to verify ownership. While some jurisdictions, such as Germany, maintain such listings in a publicly available manner, there are others where this information is not available. This presents a significant challenge to any financial institution to be able to ascertain the true ownership of entities.

In conclusion, there are a number of significant challenges with banking PEPs. The principal challenge is one of identification. This paper provides a sampling of the challenges faced by institutions in identifying who is considered a PEP. Regulators have given institutions guidance that they should apply a risk-based approach. One of the best ways to consistently develop such an approach is to have open dialog between the involved parties. This SAR Activity Review, as well as the Bank Secrecy Act Advisory Group ("BSAAG"), are examples of that dialog. By openly discussing the challenges faced by institutions, all parties stand to benefit from developing realistic and achievable expectations for what the financial community can do to prevent the scourge of public corruption. Recognizing that a risk-based approach is the best way to address this issue, the discussion should focus on several factors that indicate the greatest risk: the amount of money involved (e.g., "grand corruption"), the jurisdictional risk of the PEP, and the ability of the PEP to access the funds in the institution. However, all of these hinge on financial institutions being able to identify those clients that are PEPs.

Politically Exposed Persons: Practical Considerations and Controls

By Michael Cho, Global Head, Anti-Money Laundering Compliance

Representing Northern Trust Financial Corporation on the Bank Secrecy Act Advisory Group

Every year, financial institutions dedicate substantial time and resources to mitigate the potentially explosive reputational and legal money laundering risks associated with political corruption. Since the term “Politically Exposed Person” or “PEP” was introduced, several groups, including inter-governmental (e.g. Financial Action Task Force), global banks (e.g., Wolfsberg Group), and the U.S. government (i.e. Section 312 of the USA PATRIOT Act), have provided further guidance on the definition of PEPs and recommendations to control money laundering risk associated with PEPs. Perhaps the seminal case involving PEP risk was Riggs Bank, which received a \$25 million concurrent civil monetary penalty in 2004 for deficient AML controls relating to PEPs, including enhanced due diligence, suspicious activity reporting, currency transaction reporting, and AML governance. Accordingly, financial institutions recognize the magnitude and importance of creating and maintaining an effective AML program that specifically includes PEP identification and risk mitigation.

With the recent political unrest in the Middle East, PEP scrutiny has re-emerged, along with economic sanctions, as a primary focus of AML due diligence. Most importantly, financial institutions understand and appreciate the risk of political corruption on the integrity of the global financial economy, and thus are committed to building and maintaining robust AML programs around PEPs. Still, there remain challenges to PEP due diligence that are inherent in the definition itself, and financial institutions continue to struggle with maintaining effective, risk-based, PEP due diligence processes that also meet regulatory expectations. This article raises just a few of the challenges facing banks today, and provides some practical considerations and suggested controls to address PEP risk.⁵⁰

50. There are several sources that discuss enhanced due diligence for PEPs, such as the Federal Financial Institution Examination Council (FFIEC) BSA/AML Examination Manual. The purpose of this article is not to necessarily repeat what due diligence to perform on PEPs (e.g., collect source of wealth), but rather to discuss practical challenges with implementing and maintaining a PEP program.

Challenges with PEPs

Defining the term “PEP”

Generally, the term “PEP” is defined consistently at a high level and involves three primary characteristics: (a) persons holding senior positions of public trust (e.g., heads of state, senior executives of government-owned companies); (b) close personal (e.g., family) or professional associates of (a); and (c) persons with authority to conduct or control transactions on behalf of a PEP.⁵¹ Thus, defining PEPs may be reduced to characterizing the profile of the potential PEP (the person’s entrusted function or title; or relation to such person) and level of control over PEP or government funds. However, the simplicity typically ends there, as each of these characterizations involves complexities and (resulting) practical difficulties in defining a PEP.

First, unlike economic sanctions programs (e.g., OFAC Specially Designated Nationals (SDN) lists), there is no uniform list of PEPs. This is understandable, as PEPs are defined primarily by their entrusted function, rather than by name. Still, banks must create a risk-based program to identify PEPs consistently on an ongoing basis. One challenge is that PEP lists do not remain static. Indeed, as political offices or regimes change, the PEP associated with that office will also change. Moreover, since no uniform term exists for when an individual ceases to be a PEP, every new regime change arguably adds a new PEP, rather than just replacing a former one. Fortunately, there are several titles or functions which are generally recognized as synonymous with the definition of a PEP, including but not limited to: heads of state or government; senior government, judicial or military officials; senior politicians; and senior executives of government controlled commercial enterprises. Nonetheless, for global organizations doing business in many countries, titles may not convey functions consistently from country to country, and identifying PEPs only by title will be insufficient. For example, what is meant by “senior politician” from country to country? Is it just recognized political parties, or does it include opposition parties and grass roots movements? Honorary Consuls are generally excluded from the definition of PEP, but what about Consulates General and Ambassadors? Should they in all cases be considered PEPs, even if in some countries those titles convey no more authority than for Honorary Consuls? And what constitutes a “close personal or professional” associate? Immediate family

51. See FFIEC BSA/AML Examination Manual (pp. 130-134, 297-300) (Wolfsberg AML Principles, “Financial Action Task Force, 40 Recommendations (Recommendation 6),” and “Section 312, USA PATRIOT Act”).

members are easily defined as PEPs, but what about more distant relatives? What defines a “close professional associate” – someone having a power of attorney seems obvious, but what about a family attorney? Should attorneys always be considered PEPs? In sum, banks generally understand that defining PEPs simply by their title is insufficient; however, for large institutions, defining PEPs exclusively by entrusted function on a case-by-case basis is not only impractical but also may lead to inconsistent PEP definition.

Where banks are doing business with foreign embassies, missions or consulates, the definition of PEP brings added complexity. With such relationships, banks may hold several accounts for the PEP entity (i.e. a foreign consulate). Does that necessitate that the bank treat every signer, regardless of title, as a PEP? Arguably, a signer on such accounts has control over government funds and thus should be considered a PEP. However, does that person present the same risk as a former head of state who is also a private banking client? What if the signer is a lower level consulate employee who also has a personal account – should the bank consider the signer a PEP for the personal account as well as for the consulate account? Should the bank consider the signer a PEP just for the consulate account? What happens when it is time for a periodic review on the consulate accounts – does the bank need to conduct a review on the personal accounts as well, even if it did not categorize the signer as an individual PEP? The number of questions surrounding PEPs is intimidating – unfortunately many of those questions begin with simply defining a PEP.

Identifying PEPs

As mentioned previously, banks cannot rely on a uniform list of recognized PEPs. Accordingly, banks must rely either on a vendor solution or manual process for identification. Often, banks do both. This may raise several challenges. First, not every external vendor defines a PEP consistently – with the difficulty in defining PEPs discussed above, it would seem impossible for all vendors to use exactly the same criteria. Nonetheless, if the vendor’s methodology for defining PEPs differs from that of the bank, the bank may find itself in violation of its own PEP policy or program. Furthermore, using an automated list to screen for PEPs will require a process (and staffing) to resolve potential PEP matches. Thus, banks with large volume (e.g., large retail banks) will be challenged to implement an expedited PEP screening filter at account opening. In such cases, the PEP screening may take place after accounts are funded, though in many cases that could be only 24-48 hours after such funding takes place. This may fit the risk profile of the bank, but does present potential risk of the PEP being identified after account opening.

To prevent this, banks may implement a PEP-identification question as part of its account opening Know Your Customer (KYC) process (including Customer Identification Program (CIP) requirements). The challenge here begins with how to even phrase the question. Indeed, if experienced bank compliance professionals struggle with identifying a consistent way to define “PEP,” how can this concept be simplified for client-facing bank personnel? For example, asking a client if she is a “senior foreign political official” or someone “entrusted with a prominent public function” may be met with blank stares. In practice, presenting clients with a PEP question may identify well-recognized PEP “categories” – such as Prime Ministers, former elected officials or judges. However, clients who do not fall within such well-known categories may misunderstand the question and thus answer in the negative. If the bank representative is herself unsure of the definition, or is not equipped to press further, the PEP may go undetected at account opening. Of course, there is always the risk with a manual process (i.e. question at account opening) that the client has the option of denying his PEP status to avoid detection. In such cases, and in the absence of employment or identification documentation to the contrary, the bank will have a difficult time detecting the PEP.

Some banks take a conservative approach and combine a manual PEP account opening process with a vendor solution after account opening. In such cases, the bank may be able to confirm the PEP answer at account opening by comparing it with the automated PEP search. However, even with this (seemingly) best practices approach, challenges may arise. The PEP question at account opening must reconcile with the vendor’s definition of PEP; otherwise, the bank may be left with two different PEP lists – one from account opening and another from the vendor’s proprietary PEP list. Furthermore, because the definition of PEP can be subjective (e.g. a PEP whose function may dictate her PEP status more than her title), the account opening PEP question may identify categories of functions that are not captured on the vendor’s list. Thus, the bank would need to update the vendor with any new PEP categories (titles, functions, etc.) to ensure that other individuals with the same profile would be identified going forward. This requires constant and consistent tracking and reconciliation with the vendor.

Risk ranking PEPs

Published guidance consistently acknowledges that not all PEPs should be risk ranked the same. Banks generally understand this, and assess the risk of PEPs consistently within the framework of their client due diligence program (e.g. taking into consideration the client's products, geography, expected transactions, etc.). However, some banks are apprehensive in assigning a lower risk ranking to a PEP, especially when considering and trying to balance their primary regulator's expectations. This may lead to an automatic high risk rating for all PEPs, notwithstanding written guidance to the contrary. For an international bank that maintains client relationships globally, the number of PEPs can be significant. If all PEPs are risk rated the same, then the bank will be challenged to create a risk-based and strategic due diligence and monitoring program that is truly focused on identifying and controlling risk.

Another challenge with risk ranking PEPs is with "indirect" PEPs. Some banks may categorize PEPs as either "direct" or "indirect." Direct PEPs would be clients with whom the bank has a direct relationship. For example, a private banking relationship with a PEP would be a "direct" PEP relationship. However, banks may also maintain relationships where a PEP is not the named account holder, but rather a signer or ultimate beneficiary on the account. In such cases, should the bank apply the same due diligence for a PEP who is not the named account holder? Where a PEP has direct control over the movement of funds, perhaps. But what about relationships where the PEP has no direct authority to control the movement of funds in the account? In such cases, the first challenge may be to even identify the PEP, as the bank's due diligence program may not require a PEP question of beneficial owners. Similarly, the bank's vendor screening for PEPs may not include beneficial owners or indirect owners on the client accounts.

There are many complexities and challenges facing banks that maintain relationships with PEPs. Most fall into the broad categories of definition, identification and risk ranking.

Recommended controls

As one would expect, no single solution or "right" program exists for PEPs. Each bank must create a PEP program that is commensurate with its own risk. Examiners understand the challenges with defining, identifying and risk ranking PEPs. The key is recognizing the inherent challenges in banking PEPs, creating a risk-based, but detailed, due diligence PEP program; and managing the expectations of auditors and examiners.

Assessment of PEP risk

As is the case with the entire AML program, addressing PEP risk begins with an assessment of PEP risk at the bank. Typically this is documented in the bank's risk assessment, or within the business unit that maintains relationships with PEPs. Because defining PEPs is often a combination of title and function, as discussed above, the bank must first understand what types of PEP relationships it maintains. This is best done with business unit partners or senior management, and usually involves taking a high level inventory of known PEPs at the bank. What general categories do the PEPs naturally fall into? Examples might be: private banking clients; embassy, mission or consulate signers; retail banking clients; ultimate beneficiaries of trusts. Where are the PEPs located or what countries do they represent? What products and services are they utilizing? Are there any particular business strategies or targeted programs for PEPs? Performing such an assessment with each business unit should provide insight into the types of relationships the bank has generally, and thus provide an initial perspective of PEP risk at the bank.

Defining and risk ranking PEPs consistently

Notwithstanding the challenges in defining PEPs discussed above, banks should create a consistent and risk-based methodology for defining and risk ranking PEPs. In particular, after reviewing its high level PEP risk assessment and inventory, banks should determine how to define a PEP, using the established guidance available from such sources as: the Wolfsberg Group; Financial Action Task Force; Section 312 of the USA PATRIOT Act; and the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual. There are some entrusted positions (e.g., heads of state, prime ministers) that can always be considered senior foreign political figures. In such cases, banks may choose to simply consider these obvious titles as PEPs in all cases to eliminate at least some of the confusion around PEP definition. Banks may also choose to include certain, less obvious, titles (e.g., consulates general, ambassadors) in its PEP definition. This will depend on the bank's risk assessment and types of accounts for such PEPs. The less ambiguity surrounding the definition of PEPs, the more likely to have a consistent approach to defining PEPs.

As mentioned earlier, banks may also define a PEP by the entrusted function. For example, if the title does not obviously convey a position of senior authority, the next level of assessment could focus on the position's function and/or authority. Regardless of title, does the person now or in the past exercise a level of control over government funds? Or is the person an advisor to a PEP regarding matters of public funds? If so,

the person would be treated as a PEP. Conversely, is the title only honorary and thus not empowered to transact with government funds? Then, even if the title does not specifically mention “honorary consul,” the bank may choose to treat the position as honorary, based on its scope, and not categorize the person as a PEP. The challenge here is to be consistent throughout the bank. Regardless of how the bank decides to define its PEPs, it should understand that merely regurgitating the published definitions of a PEP in bank policy may only lead to more confusion down the road. Banks should consider such definitions in collaboration with its risk profile and make the necessary interpretations as to whom it will consider a PEP by definition.

As is the case with defining PEPs, banks should be consistent in risk ranking PEPs. Once the bank has determined a client is indeed a PEP, it will need to apply its risk ranking methodology to the PEP, utilizing such factors such as geography, products, etc. However, banks should also consider factors that may be unique to PEPs, such as the level of control over government funds, the validity of any negative news on the PEP, whether the PEP is also a signer on a government account, etc. In this way, the bank may find it easier to differentiate the risk between different PEPs – for example, a private banking PEP from a high money laundering risk jurisdiction might be considered high risk, while a junior level consulate employee who is a signer on a consulate account at the bank might be considered moderate. Again, consistency will be critical to maintaining an effective PEP program. For banks with larger PEP populations, it may be prudent to consider PEPs as a specialized due diligence category, as opposed to applying standard due diligence scoring to them. Then, as PEPs are identified, they can receive a risk ranking that takes into consideration factors unique to PEPs, which will likely produce a more risk-based PEP population. This will, of course, depend on the risk profile of the bank.

As compliance officers are well aware, however the bank decides to define and risk rank its PEPs must be documented clearly and consistently.

Training

Bank compliance officers need to collaborate with client-facing business partners to create a robust PEP due diligence program. Since there are a number of challenges in identifying and defining PEPs, business unit personnel must understand the definition of PEP and what risk factors are important. There are no new or novel approaches here – compliance officers must engage client-facing business partners and discuss the PEP program. That being said, there are obviously different training methods which can be utilized. For large institutions, online training has become the norm. However, with complicated topics (such as PEP due diligence), banks

may want to supplement such online training with smaller, targeted sessions to more fully explain the risks of PEPs to client-facing business partners. Once business partners understand the risks associated with PEPs, and perhaps walk through specific scenarios on PEP identification and risk with their compliance officers, they will be better equipped to follow the documented PEP procedures. Conversely, if they are merely presented with documented procedures to follow without truly understanding the risk, they will likely manage fine on obvious PEP scenarios, but may miss unique or truly higher risk scenarios due to a lack of understanding of PEP risk. Compliance officers should see this as an opportunity to partner with the businesses they support, as opposed to merely acting as policy creators.

Manage Expectations

Finally, compliance officers need to manage expectations of auditors and regulators. This is accomplished through early engagement, constant communication and transparency. As compliance officers are creating, revising, or even reviewing the PEP program, they may want to include internal audit partners in the discussion. The purpose is not to undermine compliance's role or authority in creating policy. Rather, the earlier compliance officers can engage and explain the rationale for their policies and procedures, the less uncertainty at the time of audit. This, in turn, will result in an audit or review that can truly focus on risk, as opposed to spending days or even weeks understanding how a PEP is defined or risk ranked. Similarly, banks should regularly communicate significant changes to the PEP program to their examination team. When engaged early in the process, most examiners will share their perspectives on risks they see in the field, and commonly will share best practices. Furthermore, just as is the case with internal audit, sharing the risk profile and rationale for the bank's PEP program early in the process likely will mean less time spent during the actual examination explaining how the bank defines and risk ranks PEPs. Again, days or even weeks can be spent just rationalizing how the bank defines PEPs, which can be frustrating for both parties.

To summarize, banks face several challenges with banking PEPs. Most fall into the category of defining, identifying and risk ranking PEPs. There is no single solution for these challenges. Rather, each bank must assess its own risk profile and make risk-based decisions on how it will choose to define, identify and risk rank. What is most important is to be consistent, to document, and to manage expectations with internal auditors and examiners.



Section 6 – Feedback Form

Financial Crimes Enforcement Network
 U.S. Department of the Treasury

Tell Us What You Think

Your feedback is important and will assist us in planning future issues of *The SAR Activity Review*. Please take the time to complete this form. The form can be faxed to FinCEN at (202) 354-6411 or accessed and completed online at <http://www.fincen.gov/feedback/fb.sar.artti.php>.

Questions regarding *The SAR Activity Review* can be submitted to sar.review@fincen.gov. For all other questions, please contact our Regulatory Helpline at 1-800-949-2732. Please do not submit questions regarding suspicious activity reports to the SAR Activity Review mailbox.

A. Please identify your type of financial institution.

Depository Institution:

- Bank or Bank Holding Company
- Savings Association
- Credit Union
- Foreign Bank with U.S. Branches or Agencies

Money Services Business:

- Money Transmitter
- Money Order Company or Agent
- Traveler’s Check Company or Agent
- Currency Dealer or Exchanger
- Stored Value

Insurance Company

Dealers in Precious Metals, Precious Stones, or Jewels

Other (please identify): _____

Securities and Futures Industry:

- Securities Broker/Dealer
- Futures Commission Merchant
- Introducing Broker in Commodities
- Mutual Fund

Casino or Card Club:

- Casino located in Nevada
- Casino located outside of Nevada
- Card Club

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).

1=Not Useful, 5=Very Useful

Section 1 - Director’s Forum	1	2	3	4	5
Section 2 - Trends and Analysis	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Issues & Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5
Section 6 - Feedback Form	1	2	3	4	5

C. What information or article in this edition did you find the most helpful or interesting? Please explain why (please indicate by topic title):

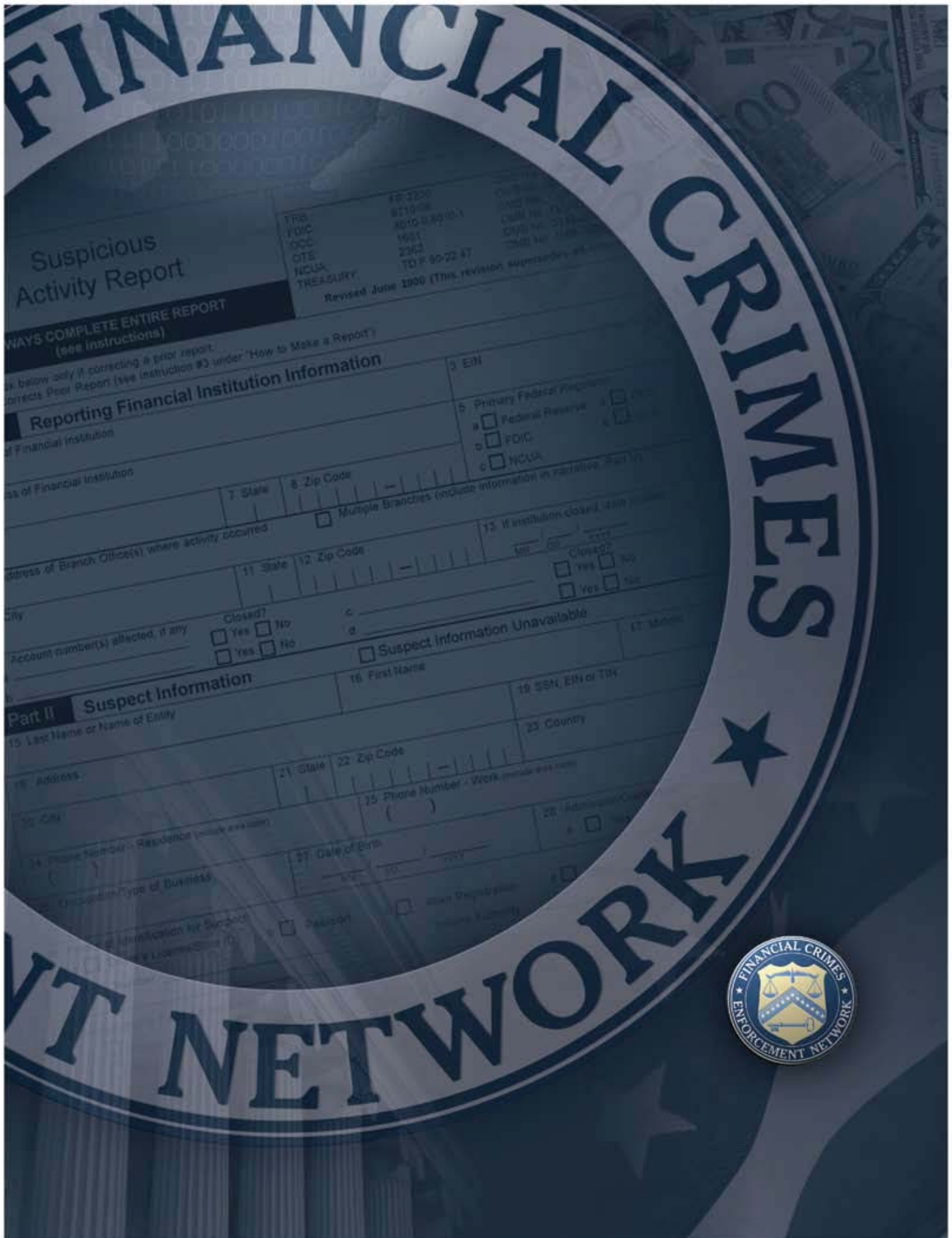
D. What information did you find least helpful or interesting? Please explain why (again, please indicate by topic title):

E. What new TOPICS, TRENDS, or PATTERNS in suspicious activity would you like to see addressed in the next edition of The SAR Activity Review - Trends, Tips & Issues? Please be specific, for example: information on a certain type of activity, or an emerging technology of interest.

F. What other feedback does your financial institution have about The SAR Activity Review publication itself?

G. How often do you read the SAR Activity Review? (Check all that apply)

- Every Issue
- Occasionally
- Only issues with content directly applicable to my industry or area of interest



FINANCIAL CRIMES

FINANCIAL CRIMES NETWORK



Suspicious Activity Report

FF 2200
821008
8010-0-8010-1
1981
2362
TDF 90-22 47
Revised June 2000 (This revision supersedes all previous editions.)
FEDERAL RESERVE BOARD
FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF THE COMPTROLLER OF THE CURRENCY
NATIONAL CREDIT UNION ADMINISTRATION
TREASURY DEPARTMENT

ALWAYS COMPLETE ENTIRE REPORT
(see instructions)

Reporting Financial Institution Information

1 Name of Financial Institution

2 EIN

3 Primary Federal Regulator
 Federal Reserve
 FDIC
 NCUA

4 Address of Branch Office(s) where activity occurred
 7 State 8 Zip Code
 Multiple Branches (include information in narrative, Part IV)

9 City

10 Account number(s) affected, if any
 Closed? Yes No
 Yes No

11 State 12 Zip Code

13 If institution closed, state reason
 Closed? Yes No
 Yes No

14 Suspect Information Unavailable

Part II Suspect Information

15 Last Name or Name of Entity

16 First Name

17 Address

18 City

19 SSN, EIN or TIN

20 State 21 Zip Code

22 Country

23 Phone Number - Residence (include area code)

24 Phone Number - Work (include area code)

25 Date of Birth

26 Occupation/Type of Business

27 Identification for Suspicious Activity Reporting (SAR) License/State ID
 Person Non-Person