PATRIOT ACT

THE CUSTOMER'S VIEW OF "KNOW YOUR CUSTOMER" — SECTION 326 OF THE USA PATRIOT ACT

*By Mark E. Plotkin & B.J. Sanford**

For the past five years, U.S. banks have devoted substantial resources to achieving compliance with provisions of the USA PATRIOT Act (Patriot Act) aimed at deterring money laundering and terrorist financing. These provisions, while directed primarily at regulated financial institutions, inevitably have impacted every person and organization that opens and maintains accounts with such institutions. As attorneys specializing in financial services regulation, we regularly receive inquiries from clients that are not financial institutions regarding what the client perceives as bizarre information requests or inappropriate conduct by financial institution counterparties. In virtually every instance, we explain that the behavior likely is attributable to the demands — or, at least, the bank's perception of the demands — of the Patriot Act.

This article discusses the most common sources of Patriot Act-related inquiries that we receive from non-financial clients: namely, the requirements of Section 326 of the Patriot Act concerning customer identification programs, and the related customer due diligence standards that regulators have imposed on banking institutions. These requirements, under the general rubric of "know your customer" or KYC, lead to periodic tugs-of-war between banks and their clients concerning the extent of the client's obligations to disclose information to the bank. This article explains those aspects of the KYC process that are visible to the customer, with a view to giving non-financial businesses a better sense of what requests they may expect from their bank, and whether such requests are reasonable.

I. Background

Within weeks of the September 11, 2001 terrorist attacks, the Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act or Patriot Act).[1] The Patriot Act contained a host of different provisions aimed at providing law enforcement and intelligence agencies the tools to deter and apprehend terrorists. Most of these provisions — such as so-called "roving wiretaps" and "sneak and peek" warrants — do not affect legitimate transactions in the ordinary

* *Mr. Plotkin is a partner, and Mr. Sanford is an associate, in the Washington, D.C. office of Covington & Burling LLP.*

1. Pub. L. No. 107-56, 115 Stat. 272.

course of business. However, Title III of the Patriot Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, introduced several new regulatory requirements for financial institutions that do indeed significantly impact many varieties of common financial transactions.

Title III amended the Bank Secrecy Act of 1970 (BSA),[2] the fundamental U.S. statute aimed at deterring and detecting money laundering, terrorist financing and other financial crimes. As originally enacted, the BSA authorized the Secretary of the Treasury to require banks to maintain certain records having "a high degree of usefulness in criminal, tax as well as regulatory investigations and proceedings."[3] Congress thereafter amended the BSA on several occasions as money laundering concerns grew during the 1980s and 1990s.[4] Title III of the Patriot Act added further requirements that had been under consideration for a number of years prior to the September 11 attacks. In addition to these specific amendments to the BSA, the terrorist attacks and the passage of the Patriot Act transformed the BSA enforcement climate and elevated the rigor with which existing BSA requirements were applied.

Its name notwithstanding, the BSA's application is not limited to banks in the traditional sense. Rather, the statute applies sweepingly to "financial institutions,"[5] a term whose statutory and regulatory definitions are extraordinarily broad, reaching businesses as diverse as casinos and precious metals dealers.[6] This article, however, focuses on the requirements specifically applicable to banks, as the vast majority of Patriot Act inquiries we receive from non-financial businesses concern banking relationships, and because, among all regulators, bank regulators have expanded the concept of anti-money laundering (AML) furthest beyond the black letter of the BSA and its implementing regulations.

---

2. Pub. L. No. 91-508, tit. I & II, 84 Stat. 1114 (codified as amended at 12 U.S.C. § 1951 et seq. and 31 U.S.C. § 5311 et seq.)

3. *Id.* at § 101.

4. *See*, e.g., Annunzio-Wiley Anti-Money Laundering Act, Pub. L. No. 102-550, tit. XV, 106 Stat. 4044 (1992); Money Laundering Control Act of 1986, Pub. L. No. 99-570, tit. I, 100 Stat. 3207.

5. A few regulations issued under the BSA apply more broadly. These regulations require any person, whether or not a financial institution, to report to the IRS (1) receipt of more than $10,000 in currency in the course of a trade or business, 31 C.F.R. § 103.30; (2) the international transportation of more than $10,000 in currency or monetary instruments, 31 C.F.R. § 103.23; and (3) interests in or control over certain foreign bank or financial accounts, 31 C.F.R. § 103.24.

6. The BSA and the Treasury Department's implementing regulations contain separate but overlapping definitions of financial institution. *Compare* 31 U.S.C. § 5312(a)(2), *with* 31 C.F.R. § 103.11(n). In practice, the following "financial institutions" are presently subject to BSA-related requirements: banking institutions, securities broker-dealers, money service businesses, casinos, futures commission merchants, introducing brokers in commodities, certain insurance companies, mutual funds, operators of credit card systems, and dealers in precious metals, precious stones, or jewels. *See generally* 31 C.F.R. Part 103.

II. KYC Generally

As noted above, the most substantial change to the business practices of the financial services industry wrought by the Patriot Act relates to "know your customer" or KYC. Like many provisions of the Patriot Act, the KYC-related measures were conceived long before the autumn of 2001. The 9/11 terrorist attacks added new political momentum to their consideration. Indeed, bank regulators first proposed a KYC regulation in 1998[7] but were swiftly forced to abandon it in the face of withering criticism from the banking industry and the public.[8]

It is the KYC process, particularly at account opening, that represents the principal Patriot Act-related friction point between financial institutions and their customers. Some customers resist providing the requested information, either because they consider it an affront or because they believe that competing financial institutions do not require similar disclosures (or, in certain instances, because they do in fact have something to hide). We routinely receive inquiries from non-financial clients as to whether a particular financial institution's request for information is justified or reasonable.

For banks, KYC has two principal components. First, pursuant to Section 326 of the Patriot Act and related regulations, banks must collect specific information from their customers and verify their identities using prescribed procedures.[9] Second, in the new regulatory atmosphere produced by the terrorist attacks and the passage of the Patriot Act, bank regulators have insisted that institutions conduct due diligence on their customers that at times goes well beyond the basic requirements of Section 326.[10]

III. Risk Assessment

The KYC regulations and guidance do not impose the same requirements on every account. Rather, banks are expected to assign a rating to

---

7. 63 Fed. Reg. 67,536 (Dec. 7, 1998) (OTS); 63 Fed. Reg. 67,529 (Dec. 7, 1998) (FDIC); 63 Fed. Reg. 67,524 (Dec. 7, 1998) (OCC); 63 Fed. Reg. 67,516 (Dec. 7, 1998) (FRB).

8. 64 Fed. Reg. 15,310 (Mar. 31, 1999) (FRB); 64 Fed. Reg. 15,137 (Mar. 30, 1999) (OCC); 64 Fed. Reg. 14,845 (Mar. 29, 1999) (FDIC); 64 Fed. Reg. 14,845 (Mar. 29, 1999) (OTS). Objection included, in the words of the OCC: "(1) [T]he regulation would be very costly to implement, especially for small banks; (2) the Know Your Customer program would invade customer privacy; (3) commercial banks would be unfairly disadvantaged and lose customers if all segments of the financial services industry are not covered; (4) compliance with the regulation would divert resources from Y2K preparation; (5) the Agencies lack authority to adopt the regulation; (6) public confidence in the banking industry would be harmed by the regulation; and (7) the regulation is both unnecessary and redundant, as banks are already familiar with their customers and have adequate procedures in place." 64 Fed. Reg. at 15,137.

9. *See* 31 C.F.R. § 103.121.

10. *See generally* Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual 56-59 (2006) ("FFIEC Manual").

each customer reflecting the risk that particular customer might conduct money laundering, terrorist financing or other financial crime through the institution.[11] This risk assessment process, which generally proceeds in accordance with a pre-established methodology devised by the bank, is performed behind the scenes. Customers rarely, if ever, learn their risk rating, nor are they generally even aware that a risk assessment is being conducted.

The risk factors that feed into a customer risk rating vary by institution. They generally include:

- Purpose of the account
- Actual or anticipated activity in the account
- Nature of the customer's business
- Customer's location
- Types of products and services the customer plans to use.[12]

Bank regulators have issued guidance discussing the risks posed by various products, locations and customer types.[13] That guidance is far too extensive to review here in full. However, as might be expected, common risk factors cited include frequent currency transactions, wire transfers and international transactions, particularly with off-shore financial centers and other "high-risk" jurisdictions.

The fact that an institution rates a customer "high risk" is not a comment on the customer's character or the legitimacy of the customer's activities. However, it does mean that, due to the nature of the customer or the customer's activities, the institution will conduct more extensive due diligence about the customer upon opening the account, and will monitor the account more closely for suspicious activities.[14] Many of these measures will be invisible to the customer, particularly if the bank never identifies any suspicious activities related to the account. Some measures, however, are more overt. For example, a business whose accounts have been rated high risk by its bank might expect one or more of the following:

- More detailed questions about its activities at account opening
- Periodic calls from bank personnel to confirm the continued validity of information given during account opening
- Requests for site visits
- Requests for information regarding individual employees or principals with control over the account
- Requests for the identity of, and information about, investors or other beneficial owners.

---

11. *See generally* FFIEC Manual at 18-27.

12. *See* FFIEC Manual at 21.

13. *See* FFIEC Manual at 163-294.

14. Banks are expected to use manual and/or automated transaction monitoring systems to identify suspicious transactions in customer accounts, with special focus on high-risk customers and activities. *See* FFIEC Manual at 61-64. They are also required to report certain suspicious activities to the Treasury Department. 31 C.F.R. § 103.18.

IV. Customer Identification Program

The cornerstone of the KYC process is the Customer Identification Program (CIP). Treasury Department regulations issued pursuant to Section 326 of the Patriot Act require every bank to implement a written CIP "appropriate for its size and type of business[.]"[15] The purpose of the CIP is to "enable the bank to form a reasonable belief that it knows the true identity of each customer."[16] The CIP procedures "must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base."[17]

As this language implies, each bank's CIP will be slightly different. However, they all require certain minimum information collection and identity verification procedures dictated by the regulation.[18] First, a bank must collect from each customer that opens a new account the customer's name, date of birth (for an individual), address[19] and identification number.[20] After collecting the information, the bank will subject each customer to an identity verification procedure.[21] This procedure may be documentary or non-documentary. Documentary verification involves examining certain identity documents. For an individual, the bank will almost always demand an "unexpired government-issued identification evidencing nationality or residence and bearing a photograph or

---

15. 31 C.F.R. § 103.121(b)(1).

16. 31 C.F.R. § 103.121(b)(2).

17. *Id.*

18. *See* 31 C.F.R. 103.121(b)(2)(i).

19. The address must be: (*i*) for an individual, a residential or business street address; (*ii*) for an individual who does not have a residential or business street address, an Army Post Office or Fleet Post Office box number, or the residential or business street address of next of kin or of another contact individual; or (*iii*) for a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location. 31 C.F.R. § 103.121(b)(2)(i)(A)(3). A civilian post office box is not acceptable.

20. The identification number must be: (*i*) for a U.S. person, a taxpayer identification number; or (*ii*) for a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. 31 C.F.R. § 103.121(b)(2)(i)(A)(4). When opening an account for a foreign business or enterprise that does not have an identification number, the bank must request alternative government-issued documentation certifying the existence of the business or enterprise. 31 C.F.R. § 103.121(b)(2)(i)(A)(4)(ii) note. A bank may open an account for a customer that has applied for, but has not received, a taxpayer identification number, provided the bank confirms that the application was filed before the customer opens the account, and obtains the taxpayer identification number within a reasonable period of time after the account is opened.

21. *See* 31 C.F.R. § 103.121(b)(2)(ii).

similar safeguard, such as a driver's license or passport."[22] For an entity, the bank will generally examine "documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument."[23] Non-documentary verification, on the other hand, "may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; [and/or] obtaining a financial statement."[24] Documentary verification is the most common practice.[25] Although non-documentary verification can serve as an alternative to documentary verification, it is often used to supplement rather than supplant the latter, particularly in high-risk or non-face-to-face transactions.

The CIP aims to verify the identity of the bank's "customer," which is defined as "a person that opens a new account."[26] Where the account is opened in the name of an entity, it is the entity — rather than its principals, investors or employees — that is deemed to be the "customer" for purposes of CIP.[27] However, based on the bank's risk assessment, it may in certain cases apply its CIP to individuals with authority or control over an entity's account, including signatories.[28] Also, even if the bank applies its CIP only to the entity customer, it still may seek information about

---

22. 31 C.F.R. § 103.121(b)(2)(ii)(A)(1).

23. 31 C.F.R. § 103.121(b)(2)(ii)(A)(2).

24. 31 C.F.R. § 103.121(b)(2)(ii)(B)(1).

25. Although the rule appears flexible on its face, the bank regulators have stated that it "reflects the federal banking agencies' expectations that banks will review an unexpired government-issued form of identification for most customers." FFIEC Manual at 48.

26. 31 C.F.R. § 103.121(a)(3)(i)(A). The term "customer" also includes an individual who opens a new account for another individual who lacks legal capacity or for an entity that is not a legal person. 31 C.F.R. § 103.121(a)(3)(i)(B). On the other hand, the following persons are excluded from the definition of customer and are therefore exempt from CIP: (1) a person that has an existing account with the bank, provided the bank has a reasonable belief that it knows the person's true identity; (2) a financial institution regulated by a federal functional regulator; (3) a bank regulated by a state bank regulator; (4) a department or agency of the United States, of any State, or of any political subdivision of any State; (5) any entity established under the laws of the United States, of any State, or of any political subdivision of any State, or under an interstate compact between two or more States, that exercises governmental authority on behalf of the United States or any such State or political subdivision; or (6) any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange, or whose common stock or analogous equity interests have been designated as a Nasdaq National Market Security listed on the Nasdaq Stock Market (except stock or interests listed under the separate "Nasdaq Small-Cap Issues" heading). *See* 31 C.F.R. § 103.121(a)(3)(ii).

27. *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090, 25,094 (May 9, 2003).

28. *See* 31 C.F.R. § 103.121(b)(2)(ii)(C).

principals, investors or employees in connection with its customer due diligence efforts.[29]

Perhaps the greatest source of CIP-related confusion between financial institutions and their customers is the CIP rule's broad definition of "account." The rule defines "account" as "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account or other extension of credit. *Account* also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian and trust services."[30] The CIP-related inquiries we receive from non-financial businesses often concern business relationships that traditionally have not been viewed as "bank accounts" in the conventional sense of the word, such as credit facilities and swap agreements. The volatile BSA enforcement climate has led banks (and, importantly, their government examiners) to be conservative, inducing many banks to subject to CIP any relationship in which the bank might be viewed as providing a service to customers.

The second greatest source of inquiries that we encounter from non-financial businesses involves the CIP rule's notice provisions. The rule requires banks to notify their customers of the CIP procedures to which the customers are subject.[31] The notice generally reads something like this:

> IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT
>
> To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.
>
> What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.[32]

Banks often incorporate such notices into customer agreements, particularly in the commercial setting. Non-financial businesses are often surprised and annoyed to find such terms inexplicably appearing in

---

29. *See* Section V, *infra*.

30. 31 C.F.R. § 103.121(a)(1)(i). The term "account" does not include: (i) a product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order; (ii) an account that the bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or (iii) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974. 31 C.F.R. § 103.121(a)(1)(ii).

31. 31 C.F.R. § 103.121(b)(5).

32. This is the text of the sample notice set forth in the rule. 31 C.F.R. § 103.121(b)(5)(iii).

agreements from which they previously were absent. This confusion is aggravated when a provision expressly references the Patriot Act, which in turn can alarm the non-financial customer.

V. Customer Due Diligence

For most banks, CIP is just the beginning of the KYC process. Banks also are required to subject each customer to a customer due diligence process (CDD) that may involve collection of a great deal more information than was gathered for purposes of the CIP. Unlike CIP, CDD is not strictly required by Section 326 of the Patriot Act. Indeed, it is not mentioned in any law or regulation, but rather is imposed on banks by their regulators as part of the supervisory process.[33]

Nevertheless, CDD as practiced today is closely connected to the terrorist attacks of 9/11, the passage of the Patriot Act, and the transformed BSA/AML enforcement climate. In this new era, the expectations of bank regulators regarding CDD have increased significantly, and the practices of banks are becoming commensurately more vigorous. In our experience, many banks, especially smaller ones, have only recently completed implementation of their CDD policies, or have yet to do so.

As noted above, the purpose of CIP is to verify the identity of the customer. The principal goals of CDD, on the other hand, are:

- To enable the bank to predict the types of transactions in which a customer is likely to engage, thus facilitating the identification of suspicious activities;
- To provide the bank with sufficient information to assign the customer a risk rating that will guide subsequent due diligence and monitoring; and
- To identify potential customers for which the risk posed by their activities, backgrounds, or sources of wealth outweigh the benefit of initiating or continuing a business relationship with them.

The specific CDD procedures a customer is likely to encounter vary widely — even more so than with respect to CIP. This is a consequence of the lack of specific elements required to be contained in a CDD program. Instead, each bank has been left to devise its own CDD program based on a mix of guidance from regulators, advice from counsel and consultants, and the lessons of its own experience. CDD procedures also are likely to

33. To the extent there is a legal basis for CDD, it most likely rests on the requirement that that a bank file a suspicious activity report whenever it "knows, suspects, or *has reason to suspect*" that certain conditions exist. 31 C.F.R. § 103.18(a)(2) (emphasis added). This objective standard for reporting means that a bank could be held liable for failure to report suspicious activity even if no one at the bank actually knew or suspected the activity was occurring or was suspicious. In order to guard against this risk, banks must monitor customer transactions for any unusual activity. However, it is difficult to identify unusual activity without knowing enough about the customer to predict the types of transactions in which the customer would normally be expected to engage. Banks gain such knowledge through the CDD process.

vary significantly by type of product or customer involved. Retail customers with transaction or credit card accounts, or commercial customers deemed "low risk" by a bank, are likely to encounter little, if any, CDD beyond the basic CIP. On the other hand, customers that bear certain high-risk characteristics or use certain high-risk products likely will face far more probing inquiries.[34]

Although it is difficult to predict precisely what information a bank will request when opening a new account, the following is a list of items that regulators have suggested may be appropriate for CDD on high-risk customers:

- Purpose of the account.
- Source of funds and wealth.
- Beneficial owners of the accounts, if applicable.
- Customer's (or beneficial owner's) occupation or type of business.
- Financial statements.
- Banking references.
- Domicile (where the business is organized).
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the customer's primary trade area, and whether international transactions are expected to be routine.
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.
- Explanations for changes in account activities.[35]

From our vantage point, the recent increase in the rigor of bank CDD policies has been a significant source of friction between banks and their customers. Some customers are understandably reluctant to disclose detailed information that would not previously have been required in connection with banking transactions. The conflict is exacerbated by the inconsistency of CDD requirements across institutions. Customers often resist providing certain information on the ground that no other bank is asking for it. Bankers, for their part, find themselves squeezed between these competitive pressures and the demands of their examiners for more rigorous due diligence. In the most difficult circumstances, bank examiners have forced a number of institutions to engage in remedial CDD projects, requiring the bank to go back to existing customers and demand information with respect to the ongoing relationship. As one might imagine, banks dread such obligations.

---

34. *See* Section III, *supra*, for a discussion of risk assessment.

35. FFIEC Manual at 57-58.

VI. Conclusion

The Patriot Act and the attendant tightening of AML controls have caused significant changes to the relationship between U.S. banks and their customers. Confusion regarding the new regulatory regime among both customers and banks has led to periodic friction regarding the disclosure of information in connection with new and existing banking relationships. This Article has sought to clarify the legal requirements and regulatory expectations underlying such bank requests for information.

For customers faced with a problematic request that the bank justifies with reference to BSA/AML compliance, it is useful to keep in mind the difference between CIP and CDD. Although the CIP regulation is not entirely black and white, customers are likely to encounter fairly uniform standards across the industry with respect to CIP. Moreover, disclosure of basic CIP information and verification of identity are non-negotiable regulatory mandates. Accordingly, it is unlikely a customer would be able to avoid disclosing the required information and presenting the relevant documents. CDD standards, on the other hand, vary widely from bank to bank (although such standards likely will converge as the industry and regulators gain more experience and develop best practices in this area.) Moreover, the regulators' CDD guidelines are relatively flexible. A bank with a well-designed CDD program, therefore, should be able to accommodate situations where its standard disclosure requirements are clearly inapplicable or impracticable, provided the bank can otherwise accomplish its objective of "knowing the customer." However, regardless of the applicable legal requirements, each bank is required to comply with its own established CDD policies and procedures, or risk possibly severe regulatory penalties. Flexibility is only possible if expressly provided by such policies and procedures.