

THE APPLICABILITY OF THE BSA/AML REGULATORY REGIME TO INDIRECT LENDING BUSINESS MODELS

Cory Howard

SUMMARY

Indirect lending, traditionally associated with the automobile industry, occurs when the retailer of an asset arranges financing for the purchaser of its goods through some type of financial institution (or alternative lender). This business model has seen extensive growth in the post-recession, low-federal funds rate banking climate, with geographic, client, and product expansion. All types of financial institutions, from large multinational banks to small credit unions have eagerly grown their indirect loan portfolios. As with most products offered by covered financial institutions, banks with indirect loan exposures need to ensure their products are part of a comprehensive and risk-based BSA/AML compliance program so that any funds extended do not become part of illicit financing schemes and the banks are not subject to regulators' enforcement actions. Since indirect lending has posed a number of challenges to finance professionals attempting to craft sound BSA/AML compliance programs, this article will walk through the reasoning and applicability of individual regulations in typical indirect lending transactions, as well as argue that some elements that are not regulatory requirements are essential for banks that wish to effectively manage compliance and reputational risk.

I. INTRODUCTION

In the world of financial regulation, one of the most heavily scrutinized areas of regulatory compliance is fulfillment of Bank Secrecy Act/Anti-Money Laundering (“BSA/AML”) obligations by financial institutions.¹ Pressure by state and federal regulators on financial institutions has increased since the 2007 financial crisis, with the U.S. Treasury adding an Enforcement Division to ensure compliance with the many

¹ Christopher Laursen, *AML Enforcement Trends*, FINANCIER WORLDWIDE (May 2014), <https://www.financierworldwide.com/aml-enforcement-trends/#WKHzQ03rsdU> (explaining the substantial fines and strict enforcement of AML regulatory requirements banks face post-2001).

statutes and regulatory requirements that comprise the framework of Anti-Money Laundering/Combating the Financing of Terrorism (“AML/CFT”) laws in the United States.² The increase in concern and enforcement actions by financial regulators is not likely a passing fad in financial regulation; in fact, it appears as if regulators will continue to press for more substantial compliance programs to mitigate what they consider years of compliance neglect.³ As a result, an increasing number of non-bank financial activities are being brought under the auspices of the BSA/AML regulatory umbrella, along with increased regulatory scrutiny of their operations.⁴ While it may seem natural that a mortgage lender, even if not operated in conjunction with traditional banking services, should be mandated to comply with anti-money laundering requirements, the Financial Crimes Enforcement Network (“FinCEN”) has also subjected limited anti-money laundering requirements on other non-financial businesses, including car dealerships.⁵ As regulatory scru-

² Sharon Brown-Hruska, *Developments in Bank Secrecy Act and Anti-Money Laundering Enforcement and Litigation*, NERA ECON. CONSULTING (June 2016), http://www.nera.com/content/dam/nera/publications/2016/PUB_Developments_BSA_AML_Lit-06.16.pdf (noting that regulatory pressure on financial institutions has been increased since the financial crisis, culminating with FinCEN, a department of the U.S. Treasury, adding a standalone compliance Enforcement Decision in 2013).

³ Marcia Savage, *Financial Institutions Reported More Suspected Fraud in 2008*, TECH-TARGET.COM (July 7, 2009), <http://searchfinancialsecurity.techtarget.com/news/1361241/Financial-institutions-reported-more-suspected-fraud-in-2008> (noting that there is a sentiment held by some in the industry that financial institutions neglected BSA/AML requirements during the financial crisis and that renewed regulatory interest in compliance will likely not fade soon).

⁴ András P. Teleki & Kathryn S. Williams, *FinCEN Extends Anti-Money Laundering Program and Suspicious Activity Reporting Requirements to Non-Bank Residential Mortgage Lenders and Originators*, K&L GATES CONSUMER FIN. SERVS. WATCH (Feb. 29, 2012), <https://www.consumerfinancialserviceswatch.com/2012/02/fincen-extends-anti-money-laundering-program-and-suspicious-activity-reporting-requirements-to-non-bank-residential-mortgage-lenders-and-originators/> (noting that the U.S. Treasury, in 2012, issued regulations requiring residential mortgage lenders and originators to develop AML compliance programs).

⁵ *Dealers Impacted by USA PATRIOT ACT Regulation*, CHICAGO AUTOMOBILE TRADE ASS'N (Nov. 23, 2010), http://www.cata.info/dealers_impacted_by_usa_patriot_act_regulation/ (noting that FinCEN had issued regulatory requirements concerning the

tiny has grown in a sector that was previously more lightly examined, federal financial regulators have begun to notice troubling trends. This includes risk-layering pertaining to underwriting, particularly in regards to collateral advances and lengthy repayment terms,⁶ which may be driven by increased competition among financial institutions.⁷ However, the risks posed by indirect lending are not all related to credit. The reduction in underwriting standards and increase in low-quality auto loans originated by dealers has increased financial institutions' regulatory risk in addition to its credit risk, mainly through reduced controls and oversight that threaten the ability of banks meet compliance responsibilities, including anti-money laundering and anti-terrorist financing regulatory standards.⁸ In fact, this article will note that even the term indirect lending is an inappropriate term for this type of lending, as it inaccurately captures the regulatory and compliance obligations of the various actors. Instead, this business model should be termed *brokered retail lending*, as that allows for proper identification of regulatory requirements for all parties involved.

Part II of this article will explore not only the history of BSA/AML regulations, but more importantly, provide an in-depth and

collection of customer information by car dealerships, as well as reporting account information to FinCEN on request).

⁶ OFFICE OF THE COMPTROLLER OF THE CURRENCY, SEMIANNUAL RISK PERSPECTIVE 5 (Spring 2015) (noting that risk-layering in commercial lending, which includes indirect dealer financing, was growing and included high LTV and liberal repayment period loans).

⁷ *Id.* at 29 (blaming increased competition among financial institutions for the reduction in underwriting standards).

⁸ Michael Corkery, *As Auto Lending Rises, So Do Delinquencies*, N.Y. TIMES, Nov. 30, 2016, <https://www.nytimes.com/2016/11/30/business/dealbook/as-auto-lending-rises-so-do-delinquencies.html> (speaking about the prevalence of “no-doc” and “false-doc” loans extended by financial institutions through indirect dealer financing programs. Altered or incorrect documents submitted by dealers to lenders not only pose substantial credit risks, but also regulatory risks, as financial institutions relying on this information cannot ensure adequate Know Your Customer compliance).

practical analysis of regulatory requirements that would be applicable to indirect lending operations. Part III will explore the application of these elements to indirect lending, with particular emphasis on this article's thesis: that channel due diligence, particularly due diligence related to third-party originations, should be considered a standard, if not required, element of any financial crimes compliance program.

II. THE HISTORY AND APPLICABILITY OF BSA/AML REGULATIONS

Common compliance terminology references the BSA/AML compliance obligations for which financial institutions are responsible. However, this is a broad set of legislative mandates and regulatory rule-making that has intertwined to create a comprehensive set of rules and regulations to which financial institutions are subject. Therefore, it is necessary for this article to break down the idea of BSA/AML compliance into smaller regulatory segments and identify which of them may be applicable to indirect lending operations. This is necessary because BSA/AML compliance has traditionally been a buck-shot approach in which attorneys and compliance officers simply throw the rule book at financial institutions' operations associates. However, the core concept of BSA/AML compliance is one of a risk-based approach, that is, that a financial institution should match regulatory obligations to methodologies of revenue generation and operations as applicable to different financial institutions, based on a myriad of factors such as the size, business model, and geographic location of the bank.⁹ While part of this article's intent is to identify some weaker points of BSA/AML compliance frameworks for *brokered retail lending* that should be modified to reduce money laundering and terrorist financing risks, this article will also serve as a compliance walk-through of brokered retail lending, a growing, but misunderstood area of the financial sector in which there is little continuity or uniformity in BSA/AML compliance.¹⁰

⁹ FEDERAL RESERVE, FEDLINKS: BANK SECRECY ACT/ANTI-MONEY LAUNDERING COMPLIANCE (Dec. 2015) (noting that BSA/AML compliance is tied to risk assessments of the bank's products, size, geography and client base and that the risks will evolve as the bank changes any of these variables).

¹⁰ This article recognizes that BSA/AML compliance is a risk-based compliance framework. When it mentioned uniformity in compliance operations that is uniformity in

A. *A Brief History of BSA/AML Regulations*

Since this article's primary focus is on the practical applications of regulatory requirements for brokered retail lending operations, it is not imperative to give a detailed history of BSA/AML regulation in the United States. However, given that the applicable regulations stem from a broader base of legislative and administrative actions, it is important to have a baseline understanding of the history of AML/CFT regulatory regime. The BSA/AML regulatory framework, as is understood today, began in 1970 with the passage of the Bank Secrecy Act¹¹ ("BSA"), which, among other things, instituted reporting requirements that necessitated banks to file Currency Transaction Reports ("CTRs") with the U.S. Treasury for transactions involving \$10,000 or more of currency, as well as collect and store information surrounding transactions of \$3,000 or more.¹² However, the passage of the BSA was not designed to stop money laundering; in fact, its purpose was to create a paper trail documenting evidence of transactions, particularly foreign transactions in countries with strict privacy laws.¹³ It was not until 1986, with the passage of the Money Laundering Control Act,¹⁴ that it became a criminal offense to launder the proceeds of criminal activities.¹⁵ Even with the

how similarity situated financial institutions would ensure regulatory compliance for similar products.

¹¹ 31 U.S.C. § 5311 (1970).

¹² Courtney J. Linn, *Redefining the Bank Secrecy Act: Currency Reporting and the Crime of Structuring*, 50 SANTA CLARA L. REV. 407, 412 (2010) (noting some of the requirements enacted by the 1970 Bank Secrecy Act, which established the first set of anti-money laundering regulations in the United States).

¹³ Jonathan J. Rusch, *Hue and Cry in the Counting-House: Some Observations on the Bank Secrecy Act*, 37 CATH. U. L. REV. 465, 471 n.33 (1988) (explaining the legislative history of the Bank Secrecy Act).

¹⁴ 18 U.S.C. §§ 1956–57 (1988).

¹⁵ Jimmy Gurule, *The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?*, 32 AM. CRIM. L. REV. 823, 823–24 (1995) (establishing the history of anti-money laundering legislation in the U.S.).

formalization of money laundering as a crime distinct from the underlying predicate criminal activity, it was not until the 1990s when financial regulators had the authority to hold banks to their BSA/AML regulatory requirements.¹⁶

The 1990s also brought the formal establishment of a government-private cooperative framework with the passage of the Annunzio-Wylie Anti-Money Laundering Act in 1992.¹⁷ With its passage, the Annunzio-Wylie Act created the Bank Secrecy Act Advisory Committee, which brought together government officials and financial industry leaders for the first time.¹⁸ In addition to the creation of the BSA Advisory Committee, the Annunzio-Wylie Act also formally mandated the detection, record retention, and reporting of potentially suspicious activity to the government (FinCEN) in the form of Suspicious Activity Reports (“SARs”).¹⁹ Even in the wake of increased public-private cooperation, however, government oversight and investigative powers were still weak. The passage of the Money Laundering Suppression Act²⁰ in 1994 strengthened financial regulators, both by giving them access to law enforcement’s information on money laundering and also by improving

¹⁶ The Annunzio-Wylie Anti-Money Laundering Act, passed in 1992, tightened the regulators’ controls over BSA/AML compliance, allowing them to regulate money services businesses and revoke the charters of federally chartered banks for convictions in money laundering or reporting requirements failures. *See* Henry B. Gonzalez, *New and Continuing Challenges in the Fight Against Money Laundering*, 20 *FORDHAM INT’L L.J.* 1543, 1545–46 (1996) (walking through the history of anti-money laundering federal legislation).

¹⁷ PETER REUTER & EDWIN M. TRUMAN, *CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING* 61, 65 (2004) (explaining the significance of the Annunzio-Wylie Anti-Money Laundering Act in furthering BSA/AML regulations in the financial industry).

¹⁸ *Id.* at 61 (noting the make-up and formation date of the committee).

¹⁹ COMM. ON NAT’L STATISTICS & COMM. ON LAW AND JUSTICE, *MODERNIZING CRIME STATISTICS* 76–77 (JANET L. LAURITSEN & DANIEL L. CORK EDs., 2016) (noting that the Annunzio-Wylie Anti-Money Laundering Act mandated that financial institutions file reports of suspicious activity with the government).

²⁰ Money Laundering Suppression Act (MLSA), 31 U.S.C.A. § 5330 (West 1994).

and fortifying the regulatory examination process of financial institutions to ensure private sector compliance with BSA obligations.²¹

Statutory and administrative rulemaking switched from anti-money-laundering to counter-terrorism in the wake of the 9/11 terror attacks.²² The passage of the USA PATRIOT Act²³ brought significant changes to the Bank Secrecy Act, from enlarging the type of businesses that were subject to anti-money laundering regulations to strengthening regulatory pressures on banks to maintain and enhance financial crimes compliance programs.²⁴ New regulations, whether statutory or administrative, have focused on increasing transparency in the financial system, such as establishing information sharing networks between banks and between banks and law enforcement²⁵ or specifying when and what types of information to collect about the beneficial owners of clients.²⁶

²¹ U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-386, BANK SECRECY ACT: OPPORTUNITIES EXIST FOR FINCEN AND THE BANKING REGULATORS TO FURTHER STRENGTHEN THE FRAMEWORK FOR CONSISTENT BSA OVERSIGHT (2006) (explaining the two objectives and major improvements of the MLSA).

²² Alvin D. Lodish, *How Well Do You Need to "Know Your Customer?"*, INFORMATION-WEEK: BANK SYST. & TECH. (Dec. 2, 2003), <http://www.banktech.com/how-well-do-you-need-to-know-your-customer-/d/d-id/1289638> (citing the shift in rulemaking policy after the 9/11 attacks).

²³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 18 U.S.C. § 2331 (2001).

²⁴ CARY STACY SMITH & LI-CHING HUNG, THE PATRIOT ACT: ISSUES AND CONTROVERSIES 48–50 (2010) (noting some of the changes made by the USA PATRIOT Act to the Bank Secrecy Act).

²⁵ These networks were established in Section 314(a)–(b) of the USA PATRIOT ACT. See also Rebekah Mintzer, *Five Laws and Regulations that Emerged from 9/11*, NAT'L L.J. (Sept. 9, 2016), <http://www.nationallawjournal.com/id=1202767045010/Five-Laws-and-Regulations-That-Emerged-From-911?slreturn=20170124131619> (citing information sharing rules as one of the regulations spurred by the 9/11 terrorist attacks).

²⁶ David McAfee, *Treasury Floats Beefed-Up Bank Transparency Rules*, LAW360 (July 30, 2014), <https://www.law360.com/articles/562717/treasury-floats-beefed-up-bank-transparency-rules> (explaining FinCEN's proposed beneficial ownership rule, which goes into effect in 2018).

B. Know Your Customer (“KYC”)

The KYC process starts with the regulatory requirements for financial institutions to develop procedures to ensure that they collect and verify the most basic of identifying information of their customers. As part of a robust Customer Identification Program (“CIP”), financial institutions must develop a way to reasonably ascertain the identity of the people with whom they do business, which includes collecting and verifying the client’s (1) name, (2) physical address, (3) taxpayer identification number, and, if the client is an individual, (4) date of birth.²⁷ However, in some instances the financial institution does not have to collect that information directly from the customer; instead, the bank can rely on the information collected from another financial institution for that customer where the second financial institution has opened an account or established similar formal banking services with the collecting bank.²⁸ However, reliance on a second financial institution is only justifiable where the reliance is reasonable, the second financial institution is subject to anti-money laundering compliance responsibilities,²⁹ and the reliance is evidenced by a written contract.³⁰ Additionally, financial institutions must only collect this type of identifying information from a customer. As defined by the regulation, a customer is a person that opens a new account, any individual who opens a new account for another that lacks legal capacity to do so, or for an entity that is not a legal person.³¹

In addition to collecting information about the identity of its clients as part a comprehensive CIP, financial institutions are required to

²⁷ 31 C.F.R. § 1020.220(a)(2)(i) (2017) (laying out the kind of information that needs to be collected and acceptable verification methods for banks to comply with the requirements of CIP).

²⁸ 31 C.F.R. § 1020.220(a)(6) (2017).

²⁹ 31 U.S.C. § 5318(h)(1) (outlining the minimum AML compliance obligations of regulated entities).

³⁰ 31 C.F.R. § 1020.220(6)(i)-(iii) (2017).

³¹ 31 C.F.R. § 1020.100(c) (2017) (defining a Customer for the CIP requirements, including carve-outs for certain entities, groups, and political subdivisions that are not considered customers and thus not subject to identity collection and verification regulations under § 1020.200).

develop Customer Due Diligence programs.³² At the very least, these programs should be comprehensive enough to allow the financial institution to understand “the nature and purpose of customer relationships for the purpose of developing a customer risk profile,” so that the institution can monitor the customer’s transactions for the purposes of detecting and reporting suspicious transactions.³³ A key part of the Customer Due Diligence requirements then is the creation of a customer risk profile, or risk rating the customer on potential money laundering and terrorist financing (“ML/TF”) risks, in order to ensure the bank is properly monitoring for and reporting suspicious activity.³⁴ Usually, to aid this transaction monitoring program, a financial institution will collect additional information from high-risk customers, usually referred to as Enhanced Due Diligence (“EDD”), to aid the bank in better understanding the client, the source of their funds, and developing a more accurate profile of what types of transactions are suspicious as opposed to routine.³⁵

C. Reporting Requirements

Another key part of the preventative anti-money laundering regulatory framework to which financial institutions are subject is a broad set of reporting requirements.³⁶ There are several different reporting obligations that financial institutions have, but two of the more prominent and

³² 31 C.F.R. §1020.210(b)(5) (2017) (establishing CDD program requirements).

³³ 31 C.F.R. §1020.210(b)(5)(i)-(ii) (2017) (establishing the goals and minimum thresholds for customer due diligence programs at federally chartered and regulated banks).

³⁴ Douglas J. Bruggeman, *Benefits of an Effective CDD Program and How Risk Scoring Customer Accounts Can Protect the Reputation of Your Institution*, ACAMS AML WHITE PAPER, INVESTIGATION, RISK ASSESSMENT, SECURITIES 7, 10–11 (noting the importance of risk scoring to guiding the transaction monitoring program).

³⁵ THE WOLFSBERG GROUP, WOLFSBERG ANTI-MONEY LAUNDERING PRINCIPLES FOR PRIVATE BANKING 6 (2012) (explaining the importance and efficacy of Enhanced Due Diligence for high-risk customers).

³⁶ RETUER & TRUMAN, *supra* note 18, at 46 (noting that reporting requirements are one of the four main components in the U.S. anti-money laundering compliance framework to which financial institutions are subject).

encompassing ones are Currency Transaction Reports (“CTRs”) and Suspicious Activity Reports (“SARs”).³⁷ Pursuant to the Bank Secrecy Act, financial institutions must file CTRs when there has been a “deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than \$ 10,000.”³⁸ A CTR must also be filed if there are multiple transactions initiated or conducted on behalf of the same person or entity, or the financial institution has reason to believe so, and those aggregations surpass the \$10,000 threshold within 24 hours.³⁹ In addition to CTR filings, financial institutions must file SARs with FinCEN when the financial institution or any employee, officer, director, or agent thereof, suspects that a transaction was or is relevant to the violation of a law or regulation.⁴⁰ These reporting requirements are heavily influenced by a financial institution’s due diligence program, as a bank’s KYC program should allow the bank to develop a profile of the customer that would allow it to determine usual behavior as opposed to potentially unusual activity.⁴¹

An essential component to any reporting requirement, therefore, is the monitoring of transactions. While not strictly mandated or specifically proscribed by BSA/AML federal regulations (although required by some state regulators),⁴² transaction monitoring is a key tool in allowing

³⁷ *Id.* at 54–55.

³⁸ 31 C.F.R. § 103.22(b)(1) (2011).

³⁹ Michael J. Parrish, *The Burden of Currency Transaction Reporting on Deposit Institutions and the Need for Regulatory Relief*, 43 WAKE FOREST L. REV. 559, 561 (2008) (explaining the aggregation requirement for filing CTRs).

⁴⁰ 31 U.S.C. 5318(g)(1) (2014); *see also* Eric J. Gouvin, *Bringing Out the Big Guns: The USA PATRIOT ACT, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955, 967 (2003) (discussing the legislative creation of the SAR and when financial institutions are responsible for filing one).

⁴¹ Előd Takáts, *Domestic Money Laundering Enforcement*, in BLACK FINANCE: THE ECONOMICS OF MONEY LAUNDERING 209 (Donato Masciandaro et al. ed., 2007) (explaining the interplay of KYC/CDD and reporting requirements).

⁴² N.Y. COMP. CODES R. & REGS. tit. 3 § 504 (2016) (requiring financial institutions to have and maintain transaction monitoring programs).

banks to identify and flag potentially unusual activity performed on a customer's account.⁴³ As a result, transaction monitoring programs are risk-based, like many of the BSA/AML program elements, and are tailored to the financial institution's customer base, product offering, and geographic reach.⁴⁴ Whether a financial institution utilizes third-party vendor software, manual review of daily/periodic reports, or builds a proprietary transaction monitoring system, the end goal should always be the same: the financial institution should be able to adequately, and within a risk-guided framework, monitor accounts, and transactions for potentially suspicious activity.

D. Sanctions Compliance

In addition to BSA/AML concerns, financial institutions (and in fact all U.S. regulated companies and individuals) are subject to compliance with economic and trade sanctions imposed by the federal government on entities, people, ports, and vessels.⁴⁵ Sanctions lists, which are maintained by a group in the Treasury Department called the Office of Foreign Asset Control ("OFAC"), are lists of designated entities with whom it is illegal for individuals or corporations within the U.S. to do business with, absent special exemptions.⁴⁶ Notably, sanctions compli-

⁴³ It is not the method of detection that is legally proscribed, only that banks report suspicious activity to the federal government. *See* 12 C.F.R. § 21.11(c) (2017) (requiring federally chartered financial institutions to file SARs with FinCEN if potentially suspicious activity is detected).

⁴⁴ FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH: THE BANKING SECTOR 21 (2014) (noting the different elements financial institutions should consider when building/evaluating a transaction monitoring program).

⁴⁵ Elsa Manzanares & Michelle Schulz, *Sanctions Compliance Issues for Non-U.S. Companies*, GLOBAL TRADE MAG. (Dec. 8, 2015), <http://www.globaltrademag.com/global-trade-daily/commentary/sanctions-compliance-issues-for-non-u-s-companies> (stating that all U.S. persons must comply with economic and trade sanctions on people, entities, vessels or locations and that OFAC is responsible for enforcement of compliance).

⁴⁶ Zachary Brez & Michael Casey, *4 Steps Towards OFAC Sanctions Compliance*, LAW360 (Aug. 12, 2011), <https://www.law360.com/articles/262952/4-steps-toward-ofac-sanctions-compliance> (explaining that OFAC maintains OFAC lists and enforces com-

ance, like most anti-money laundering requirements, is also risk-based, and financial institutions are given some leeway in implementing programs based on the bank's risk factors.⁴⁷ Although OFAC maintains a list of prohibited entities, it does not mandate how financial institutions should comply with the requirement to not do business with sanctioned entities; instead, it directs financial institutions to the FFIEC for guidance.⁴⁸

As a standard practice within the industry, financial institutions utilize sanctions screening to ensure that they are not transacting business with listed entities, and so that they can adequately disposition the transaction in the case of a positive match. This involves screening the names of the parties, entities, and vessels involved in a given transaction. These screens can be transactional, such as when a payment is processed or an outbound wire is sent, or on a party-based approach for those who may be involved in repeat transactions, or a combination thereof. Additionally, financial institutions usually preemptively screen potential clients, vendors, employees, and other third-parties before engaging in business or opening accounts, as well as conducting periodic checks of those parties against OFAC's sanctions lists to ensure that no party within whom the bank engages has been placed on a sanctions list.⁴⁹

pliance and that U.S. individuals and corporations cannot transact with listed countries or entities, absent special permissions/circumstances).

⁴⁷ 31 C.F.R. pt. 501, app. A (2016) (noting that the bank's compliance program should be tailored to its "size, customer base, business volume, and product types"). Risk-based, in the context of AML and OFAC compliance, refers to the structure of subject person's programs, not in adherence to the actual regulations themselves.

⁴⁸ Jeremy P. Panner, *No Sanctions Compliance Program? Expect Significant Penalties*, THE NAT'L L. REV. (July 27, 2016), <http://www.natlawreview.com/article/no-sanctions-compliance-program-expect-significant-ofac-penalties> (explaining the lack of prospective compliance obligations from OFAC).

⁴⁹ Louis Rothberg et al., *OFAC Cites Violations in Dealing with Specifically Designated Nationals*, THE NAT'L L. REV. (Aug. 5, 2016), <http://www.natlawreview.com/article/ofac-cites-violations-dealings-specially-designated-nationals> (recommending as an industry standard that financial institutions screen initially and periodically its clients, employees, contractors, and payees to ensure that it is not transacting with an entity on one of the OFAC lists).

III. THE FINANCIAL REGULATORY FRAMEWORK OF BROKERED RETAIL LENDING

One important feature of BSA/AML regulatory requirements is that they are risk-based, that is, financial institutions are charged with identifying, properly assessing, and understanding potential money laundering and terrorist financing risks their operations may pose and enacting a compliance program that mitigates those risks.⁵⁰

Compliance with anti-money laundering and terrorist financing regulations is a tailored approach that differs for every financial institution, based on factors such as geographic reach, customer base, and product offerings.⁵¹ Given the particular emphasis on risk inherent in the BSA/AML compliance regulatory regime, it is imperative that requirements are crafted around the financial institution's risk profile, which necessarily indicates that different product lines are identified and risk-rated. One product line that is prevalent in a number of banks but is consistently misunderstood is commonly referred to as "indirect lending," which this article asserts should be referred to as *brokered retail lending*.

A. *What is Indirect Lending?*

Indirect lending is a form of financing in which a financial institution lends money for the purchase of consumer goods through a third-

⁵⁰ FIN. ACTION TASK FORCE, *supra* note 45, at 6 (noting that compliance with money laundering/terrorist financing regulatory requirements is not a scatter-shot, but a risk-based approach. This requires the financial institution to understand its operations and tailor a program around those operations instead of simply sticking to a standard one-size-fits-all playbook that may not fit the risk profile of the bank's customers or products).

⁵¹ FED. FIN. INSTS. EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 23 (explaining that financial institutions must identify relevant risks in order to craft a comprehensive BSA/AML compliance program that meets the financial institution's risk profile).

party, who is usually the seller of the goods being purchased.⁵² An example of an indirect loan would be financing through an auto dealership: when a borrower completes a loan application at a car dealership, the dealer farms out the application to lenders, and the lender returns to the dealer with an approval for the parameters of the proposed sales agreement between the borrower and dealer.⁵³ Financial institutions build these programs by cultivating relationships with auto dealers. Sometimes there may be pre-set parameters set by the financial institution and given to intermediary solutions used by dealers that define what type of borrower will be underwritten by the financial institution and the proposed terms of the loan.⁵⁴ This type of lending, particularly as it pertains to auto dealer financing, is important to recognize given that it now accounts for 56% of all auto lending for some types of financial institutions.⁵⁵ While indirect auto lending has gained significant traction with credit unions, large financial institutions also have large auto loan portfolios, with a large percentage of those portfolios generated through indirect financial arranged by a dealer.⁵⁶ Not only do financial institutions need to recognize the risk profile that continually-growing indirect lend-

⁵² Tim Melrose & Karin Modjeski Bearss, *Indirect Lending: Safety and Soundness*, FED. RESERVE BANK OF MINNEAPOLIS (Dec. 2014), <https://www.minneapolisfed.org/publications/banking-in-the-ninth/indirect-lending> (defining indirect lending).

⁵³ Charles Goss, *How Indirect Lending Can Really Work*, CREDIT UNION TIMES (Mar. 2, 2014), <http://www.cutimes.com/2014/03/02/how-indirect-lending-can-really-work> (illustrating a common form of indirect lending, i.e. lending facilitated by an auto dealership).

⁵⁴ James A. Wilson, Jr. et al., *The Changing Landscape of Indirect Automobile Lending*, FDIC SUPERVISORY INSIGHTS (Summer 2005), https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum05/article04_auto_lending.html.

⁵⁵ Greg Gonsalves, *Indirect Lending at Year-End 2016*, CREDITUNIONS (Feb. 13, 2017), <http://www.creditunions.com/blogs/industry-insights/indirect-lending-at-year-end-2016> (noting the year-over-year increase in indirect auto lending as a percentage of the total auto loan portfolios of credit unions).

⁵⁶ Jessica Silver-Greenberg & Michael Corkery, *In a Subprime Bubble for Used Cars, Borrowers Pay Sky-High Rates*, N.Y. TIMES (July 19, 2014), https://dealbook.nytimes.com/2014/07/19/in-a-subprime-bubble-for-used-cars-unfit-borrowers-pay-sky-high-rates/?_r=0 (noting that out of Wells Fargo's \$52.6 billion car loan portfolio in 2014, a majority of those loans originated through dealerships).

ing profiles carry, but also the inherent product risk they carry, such as trade-based money laundering involving the purchase of cars, especially luxury cars.⁵⁷

Not only do financial institutions need to be aware of the inherent risks in indirect lending, magnified by the growth of the product, but the risk of the customers is particularly important as well. In recent years, financial institutions have increasingly turned to subprime lending,⁵⁸ or lending to borrowers with credit scores defined as subprime,⁵⁹ in the hopes of replacing profits squeezed as a result of low interest rates.⁶⁰ Subprime consumers obviously pose greater credit risks than prime customers,⁶¹ hence the higher interest rates,⁶² but subprime (and indirect)

⁵⁷ Nick Bunkley, *Export Scammers' Gain is Dealers' Pain*, AUTOMOTIVE NEWS (July 1, 2013), <http://www.autonews.com/article/20130701/RETAIL07/307019970/export-scammers-gain-is-dealers-pain> (noting the prevalence of and explaining how export based financial crimes operate as it relates to the automotive industry).

⁵⁸ Jennifer Taub, *The Subprime Specter Returns: High Finance and the Growth of High-Risk Consumer Debt*, NEW LABOR FORUM (Dec. 28, 2015), <http://newlaborforum.cuny.edu/2015/12/28/the-subprime-specter-returns/> (noting that financial institutions have increasingly turned to subprime lending in the years after the 2007 financial crisis, particularly subprime auto lending, as these loans require down payments and are secured by collateral).

⁵⁹ Todd J. Zywicki & Joseph D. Adamson, *The Law and Economics of Subprime Lending*, 80 U. COLO. L. REV. 1, 17 n.68 (2008) (explaining that a subprime borrower, as determined by FICO, is a borrower with a credit score under 620).

⁶⁰ Taub, *supra* note 58 (linking the rise of post-financial crisis subprime borrowing to decrease in profits of other bank products).

⁶¹ Andre K. Gray, *Caveat Emptor: Let the Borrower Beware of the Subprime Mortgage Market*, 11 U. PA. J. L. & SOC. CHANGE 195, 199 (2007-2008) (tying subprime borrowers to greater credit risks and risks of default); *see also* AnnaMaria Andriotis, *Subprime Auto-Loan Loss Expectations Rise*, WALL ST. J. (July 12, 2016), <https://www.wsj.com/articles/subprime-auto-loan-loss-expectations-rise-1468341801> (noting the rise in subprime auto loan delinquencies).

⁶² Steve Hoke, *The Risks and Rewards of Sub-Prime Auto Lending*, CREDIT UNION MAGAZINE (Dec. 19, 2015), <http://news.cuna.org/articles/108484-the-risks-and-rewards-of-subprime-auto-lending> (noting that there is a \$4,626 revenue difference between a 60-

loans are particularly susceptible to fraud and money laundering, likely due to economic instability.⁶³

Even beyond the realm of subprime auto lending and the financial problems those borrowers face, origination channels for indirect lending are particularly susceptible to fraud, which can include, or mask, money laundering. Since the principle origination channel for indirect lending is through the asset's retailer, there is built in incentive for fraud. Of the possible types of fraud, brokered retail lending is subject to include: falsification of documentation for credit application,⁶⁴ deceptive fee practices,⁶⁵ outright money laundering through cash payment discounts, and structuring.⁶⁶ In fact, financial institutions have been accused of either negligently ignoring potential bad actors or of turning a blind eye to their behavior in the face of increased revenue.⁶⁷ While federal

month super prime loan [issued at 3.53% interest] and a sub-prime loan [issued at 14.15% interest] for lenders). The increased interest rate to sub-prime borrowers is to compensate for the credit risk the financial institution takes in lending to a less-stable borrower who is statistically more likely to default on the loan.

⁶³ FBI, MORTGAGE FRAUD REPORT 2007 (2008) (noting that the growth in subprime mortgagees continually edged up the mortgage fraud rate in 2007); see also LARRY J. SIEGEL & JOHN L. WORRALL, ESSENTIALS OF CRIMINAL JUSTICE 334 (9th ed. 2013) (linking the increase in subprime mortgage lending to the increase in mortgage fraud).

⁶⁴ Jessica Silver-Greenberg & Michael Corkery, *Loan Fraud Inquiry Said to Focus on Used-Car Dealers*, THE NEW YORK TIMES (Oct. 1, 2014, 10:00 PM), <https://dealbook.nytimes.com/2014/10/01/loan-fraud-inquiry-said-to-focus-on-used-car-dealers/> (noting that ongoing state-level investigations have found numerous suspected cases in which dealerships falsified loan information/documentation).

⁶⁵ Rachel Abrams, *Dealer Fees for Arranging Car Loans Are Drawing Scrutiny from U.S.*, N.Y. TIMES (Nov. 22, 2013), https://dealbook.nytimes.com/2013/11/22/scrutiny-over-disparity-in-loan-fees-at-auto-dealerships/?_r=0 (explaining that hidden dealer fees, including financing fees, are under regulatory scrutiny).

⁶⁶ Kieran Nicholson, *Commerce City Car Dealer Nets 4 Year Prison Term for Money Laundering*, DENVER POST (Dec. 1, 2015), <http://www.denverpost.com/2015/12/01/commerce-city-car-dealer-nets-4-year-prison-term-for-money-laundering/> (reporting that a Denver area car dealer had pled guilty to money laundering and structuring charges).

⁶⁷ Deirdre Fernandes, *Mass. AG Probes Santander for Auto Lending Practices*, THE BOSTON GLOBE (Dec. 25, 2014), available at <https://www.bostonglobe.com/business/2014/12/25/investigates-santander-for-auto-lending-practices/RK51H7I83Bd2Uxrr>

bank regulators, such as the Office of the Comptroller of Currency (“OCC”) have issued strict requirements for vendor oversight and controls, this is a risk-based approach that requires active identification of vendor relationships, third-party services performed, and rating for identifying at-risk relationships.⁶⁸ This type of risk management is appropriate and necessary for non-vendor third-party relationships, but the lack of a formal regulatory program for BSA/AML compliance, as it pertains to third-party assisted, indirect lending, hampers the ability of financial institutions across the industry to develop a comprehensive and somewhat uniform approach. Given the potential risks posed by indirect lending operations, both from subprime borrowers and relationships with auto dealers, it is imperative that financial institutions recognize, rate, categorize, and mitigate the money laundering and terrorist financing risks that these pose in a manner that allows the financial institution to continue profitable operations while ensuring regulatory compliance and the integrity of the financial system.

However, the traditional retail-generation methodology for indirect loan origination is no longer the sole source for creating indirect loan portfolios. Instead, financial technology companies (“fintechs”) are beginning to wade into the waters of indirect lending by generating customers and routing them to financial institutions. Following the “search-click-apply-fund” mantra, prospective borrowers may be able to search a list of funding institutions offering loans within pre-set parameters, choose the one with the most suitable product offering, apply through the on-line origination platform, and have the chosen financial institution

CFeSLM/story.html (noting that Santander had settled a lawsuit in which the plaintiffs alleged that Santander failed to monitor a New York dealership in which an employee falsified loan documents).

⁶⁸ OFFICE OF THE COMPTROLLER OF THE CURRENCY, THIRD-PARTY RELATIONSHIP RISK MANAGEMENT GUIDELINES, OCC BULLETIN 2013-29 (2013) (in which the OCC calls for stricter oversight of third-party relationships by financial institutions, including the completion of due diligence and having robust contracts that ensure compliance).

fund the loan.⁶⁹ Often aimed at improving the retail car buying process, fintechs capture and validate loan information before the customer gets to the dealer (or instead of having the customer go to a financial institution, in the case of auto loan refinancing) and pass the completed application along to the chosen funding institution.⁷⁰ While the auto loan process has had a digitized component since the early 2000s, with the emergence of prominent financing tools, such as DealerTrack and Route One,⁷¹ new fintechs are a twist on an older process. Instead of working in conjunction with auto dealers to process applications and match borrowers with potential lenders, newer fintechs aim to simplify the auto buying or refinance process and instead match customers with lenders before the purchaser sets foot on an auto lot.⁷² This, however, poses a new set of regulatory obstacles for funding institutions linked to their customers through this type of fintech.

B. *BSA/AML Compliance Obligations in Indirect Lending*

Ultimately, the method of origination, while important, does not change the fact that financial institutions, whether large banks or credit unions, fund the loan. If a financial institution chooses to offer this product line, it is required to develop some type of financial crimes compliance program to ensure that applicable BSA/AML regulatory burdens are met. The rapid growth in the customer base, the evolving methods of loan origination, and the propensity for vehicles to be used in money laundering and terrorist financing, make it imperative that financial institutions

⁶⁹ Press Release, MoveCU, Inc., Credit Union Fintech Merges Indirect and Direct Lending Processes (Sept. 9, 2016), <https://www.cuinsight.com/press-release/credit-union-fintech-merges-indirect-direct-lending-processes> (explaining the operations of a fintech start-up that has become a customer generator for indirect lending).

⁷⁰ Zack Miller, *Car Companies Look to Fintech to Fund New Lending and Finance*, TRADE STREAMING (Jan. 26, 2017), <http://www.tradestreaming.com/digital-lending/car-companies-look-to-fintech-to-fund-new-lending-and-financing> (noting “Online financing tools capture and validate an applicant’s complete information when applying for a loan”).

⁷¹ *Id.* (noting that eOriginal, a digital financing company, has had two products on the market since the early 2000s, Dealer Track and Route One, which match lenders with customers).

⁷² *Id.*

develop a robust compliance program for indirect lending products. Most AML compliance programs related to indirect lending are applied on a bank-wide system, so three of the four pillars of AML compliance, (1) the appointment of a BSA/AML compliance officer, (2) appropriate training for employees, and (3) independent testing, should already be in place.⁷³ In regards to the three mentioned pillars (and even as to the newly enacted fifth pillar),⁷⁴ indirect lending will predominately be the same as most other product types. However, one of the pillars, a system of internal controls, should look substantially different and have intricacies and related problems not seen in other product lines. So what exactly would such a program look like for this particular type of product?

1. Know Your Customer

a. Customer Identification Program

An essential part of any financial institution's internal AML controls are those relating to the Know Your Customer requirements. One of the key components is the creation of a Customer Identification Program ("CIP") in which four major pieces of information are collected from the customer: (1) name, (2) physical address, (3) taxpayer ID, and for natural persons (4) date of birth.⁷⁵ For indirect lending, the customer is the borrower for whom the loan is being extended, not the auto dealer.

⁷³ Maria A. de Dios, *The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy*, 10 BROOKLYN J. CORP. L. & FIN., 495, 504 (2016) (listing and explaining the "Four Pillars" of an effective AML/CFT compliance regime).

⁷⁴ FinCEN has recently instituted new regulations establishing a "Fifth Pillar" of AML/CFT compliance: the collection of beneficial ownership, down to those holding a 25% ownership stake in the client or those that have a substantial say in operations. However, since this rule is not slated for enforcement until May 11, 2018 this article will not discuss it. See Jacquelin M. Allen, *Inside FinCEN's Beneficial Ownership Final Rule*, LAW360 (May 26, 2016), <https://www.law360.com/articles/800744/inside-fincen-s-beneficial-ownership-final-rule> (discussing the timing and content of FinCEN's Fifth Pillar).

⁷⁵ 31 C.F.R. § 1020.220(a)(2)(i) (2017) (listing the information required to be collected as part of a CIP).

Frequently, if not exclusively, in indirect lending, the financial institution extending credit (and thus the entity responsible for collecting and verifying customer information) is not the entity that has contact with or processes the applicant's information. Instead, the dealer (or fintechs, for non-dealer loan originations) is the entity/application that serves as a conduit for the customer's information. For example, a typical transaction would start with the customer choosing a vehicle at an auto dealership, the applicant filling out a loan application (usually a dealer proprietary application), and the dealer inputting the application information into an application such as Dealer Track or Route One, which then finds potential lenders. These lenders perform initial underwriting on the loan based on the information provided and decision the borrower while creating the terms of the loan. As a result, many financial institutions rely on the identity collection/verification procedures of auto dealers, as permitted by subsection 6 of the CIP regulation.⁷⁶ Unlike Customer Due Diligence ("CDD"), which is performed after account opening, CIP must be performed prior to account opening, with clear instructions on when a customer's inability to document or verify their identity should lead to a refusal to open an account.⁷⁷ Therefore, financial institutions relying on common methods of indirect funding must ensure that they can rely on the identity collection/verification procedures of dealers. Since auto-dealers are regulated and required to collect CIP from customers, financial institutions need only to ensure that there is a valid contract between the two parties certifying that the collecting party annually certifies its anti-money laundering program and that it is performing CIP on the financing bank's behalf.⁷⁸ As a result, the only question lending institutions need to answer is whether its reliance on the auto dealer is

⁷⁶ 31 C.F.R. § 1020.220(a)(2)(ii)(6) (2017) (permitting financial institutions to rely on the identity collection/verification procedures of other entities where such reliance is: (i) reasonable, (ii) the financial institution is subject to BSA/AML regulations, and (iii) there is a written contract between the two parties clearly delineating the roles and responsibilities of the parties).

⁷⁷ 31 C.F.R. 1020.220(a)(2)(iii) (2017) (noting that a financial institution must have procedures dictating when the bank should not open an account if it cannot collect the requisite information to form a reasonable belief as to the identity of its customer).

⁷⁸ 31 C.F.R. 1020.220(a)(2)(ii)(6)(iii) (2017).

reasonable. That question, however, can only be answered by the next set of BSA/AML control indirect lenders need: Customer Due Diligence.

b. Customer (and other) Due Diligence

Another important piece of any robust KYC program is Customer Due Diligence. During the due diligence phase, the goal of the financial institution is to form a more complete picture of their potential client in order to risk rate their clients, that is, to determine whether and which clients pose an increased risk for money laundering or terrorist financing.⁷⁹ Once the clients have been identified and risk-rated, the financial institution then must develop a risk-based approach to ensure that it can distinguish and report potentially suspicious activity.⁸⁰ In indirect lending, though the origination channels may differ from traditional retail lending operations, the “customer” is usually the borrower.⁸¹ As a result, any CDD required as part of a risk-based program would include the collection of additional information beyond that collected during CIP that would allow the indirect lender to receive a more complete view of the borrower and their expected activity. Ultimately, it is the borrower’s transaction history that will be under scrutiny and the one that the lending institution will need to monitor and report on.⁸² In the world of indirect lending, CDD or EDD, if the lender is dealing with all high-risk

⁷⁹ BASEL COMM. ON BANKING SUPERVISION, SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND THE FINANCING OF TERRORISM 4 (2016) (explaining the practical purpose behind the collection of information during CDD is to better understand, rate, and monitor customers for potentially unusual activity).

⁸⁰ *Id.*

⁸¹ This article has adopted the regulator’s definition of customer, that is, one who opens a new account either for themselves or on behalf of someone else who lacks the capacity to do so (such as a minor, or an entity that is not a legal person such as a civic club). *See* 31 C.F.R. §1020.100(c)(1) (2017). There may be some derivations in this formula, for example, if dealers execute and fund installment sales contracts, which are then purchased by financial institutions.

⁸² *Id.* at 6.

clients (typically, a solely sub-prime business model concern) or has rated a client as having an elevated ML/TF risk, the process is paper-intensive, but tends not harm business prospects.⁸³ This type of CDD/EDD may include verifying employment, verifying accuracy of stated pay, verifying previous address, etc., either through documentary or non-documentary means.⁸⁴ While the collection of information required for CIP can be accomplished through reliance on another bank, financial institutions cannot outsource risk rating and CDD information gathering/EDD to the originating party.⁸⁵ Instead, the financial institution must perform these functions itself. For best practices, the financial institution should be sure not just to collect the information, but to also thoroughly verify the information, given that it may have to pass through multiple parties to get to the financial institution in the first place.

c. Information Refresh

A key part of any CDD compliance regime is not only knowing, identifying, and monitoring high-ML/TF customers of financial institutions, but also keeping the information required for subsequent monitoring programs up-to-date. This is especially important with accounts that have open-ended or medium- and long-term life cycles. FinCEN has explicitly enumerated the need for a compliance program that not only performs due diligence on client during onboarding, but that has systems in place to make sure updated client information is collected during the

⁸³ E.g., Jim Henry, *How Some Customers Cheat Themselves*, AUTOMOTIVE NEWS (Nov. 5, 2014), http://www.autonews.com/article/20141105/FINANCE_AND_INSURANCE/311059995/how-some-customers-cheat-themselves (discussing alternate documentation and verification procedures performed by auto dealers that more accurately allows them to determine the identity and other information about potential buyers without reducing business prospects).

⁸⁴ Although this information is usually collected during the underwriting stage, financial institutions may “double-count” it as long as the information is being input into a risk rating that factors ML/TF risk. See Lou Loquasto, *Driving in the Fast Lane with Instant Income and Employment Verification*, NONPRIME TIMES (NOV.-DEC. 2013), <http://www.theworknumber.com/go/News/NPT-EVS-article.pdf> (noting common data points and information sources used during credit indirect lending underwriting, and thus available for ML/TF risk rating).

⁸⁵ See 31 § C.F.R. 1020.220(a)(2)(ii)(6) (2017).

life of the account.⁸⁶ As a result, financial institutions are charged with ensuring that active accounts are not tied to stagnant client information, such as outdated addresses or incorrect names. Many financial institutions usually require periodic collection of basic CIP information from clients during first contact with an associate after a set period has passed, typically one to two years since the last update. However, in a brokered retail lending relationship, the periodic refresh of information may be more difficult to ascertain. While the financial institution is ultimately required to collect such information, it is entirely possible that the client will not contact the lender during the course of a three to six year auto loan, aside from making payments (which can be made predominately online).

Traditionally, it is easier to refresh customer information in the context of a broader banking relationship, such as where there is a deposit account/mortgage loan, as both will more likely require the account holder to be in contact with the financial institution's associate for routine account maintenance. However, brokered retail lending carries no such guarantees. Compounding this problem is the tenuous nature of the client relationship, as it is the auto-dealer or fintech that is responsible for origination and who may sometimes be the party that owns and is responsible for maintenance of the client relationship. As a result, the financial institution holding the lending relationship needs to ensure that it has processes and procedures in place to refresh its customers' identifying information over the course of the loan so that it can guarantee that the bank has an accurate picture of the client's usual course of transactions, including any changes to the client's geographic, economic, or personal circumstances.

⁸⁶ Jack Baughman et al., *FinCEN Issues Sweeping New Requirements on Collection of Beneficial Ownership Information and Customer Due Diligence*, LEXOLOGY (May 10, 2016), <http://www.lexology.com/library/detail.aspx?g=6eb541d5-570e-4650-8ebe-1931e5a7f86a> (noting that a key part of FinCEN's "Fifth Pillar" [CDD] is the refresh and continued collection of information from active clients).

2. Regulatory Reporting and Transaction Monitoring

Indirect lenders are also responsible for reporting requirements, and intermediate transaction monitoring, which may be made more difficult because of the method of origination.⁸⁷ While fintech and dealer originated loans should not, in theory, pose problems for the lenders to monitor accounts, it is possible that the lending institution may have limited oversight over the originator. In a brokered retail arrangement, dealers and fintechs would only be responsible for origination, with account servicing, including payment processing, performed by the lender.⁸⁸ However, there can be potential roadblocks to accurate transaction monitoring and regulatory reporting if the client relationships, and consequently, CDD/Risk rating processes, are performed by the originator without duplication by the lender. Whether there is a contractual relationship between the originator or financial institution stipulating the sharing of information surrounding the client or strong vendor/channel oversight on the part of the financial institution, the lender needs to ensure it has the information necessary to form an accurate picture of the client and the type of account activity that is usual.⁸⁹ If there is a bifurcated client relationship, the financial institution needs to ensure that it has adequate oversight of the vendor to ensure it has the information that it needs. This can include, among other things, employees dedicated to working with vendor controlled accounts, daily and monthly transaction reports reviews, and periodic receipt of information reported by the vendor to the lender, or risk scorecards filled out by the vendor to keep

⁸⁷ *Id.*

⁸⁸ Although loan servicing could be, and in the case of smaller financial institutions, is outsourced to a third-party servicer, that relationship is outside the parameters of brokered retail lending and is subject to its own oversight compliance obligations. OFFICE OF COMPTROLLER OF CURRENCY, OCC BULLETIN 2013-29, RISK MANAGEMENT GUIDANCE (Oct. 30, 2013), <https://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>.

⁸⁹ *Id.*

the financial institution informed on the compliance risks associated with the portfolio of clients it owns or loans it services.⁹⁰

C. The Importance of Channel Due Diligence and Third-Party Oversight

In an increasingly complex financial system, financial institutions have and continue to rely on an extensive network of vendors and third-party relationships to, among other functions, develop and operate lines of business, identify and on-board potential customers, and perform core bank functions, such as IT or legal service providers.⁹¹ This trend towards outsourcing key functions continues to pose substantial risks for banks, from a legal, compliance, reputational, and business continuity perspective.⁹² Recently, there has been increased scrutiny from regulators and organic vendor management efforts by financial institutions to make sure these relationships are operating according to regulatory guidelines and in accordance with the banks' core values and mission statements.⁹³ As a result, concrete risk management principles have been developed by banks internally, and also issued by regulators, that provide an extensive playbook by which to ensure that third party relationships, although not strictly vendor based, which dominate the field of indirect lending, are appropriately managed.⁹⁴

⁹⁰ Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29,398, 29,422 (May 11, 2016) (to be codified at 31 C.F.R. pt. 1010, 1020, 1023, 1024, and 1026).

⁹¹OFFICE OF COMPTROLLER OF CURRENCY, OCC BULLETIN 2013-29, RISK MANAGEMENT GUIDANCE (Oct. 30, 2013), <https://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html> (noting some of the functions that have been shifted from in-house responsibility to performance by vendors and third-parties).

⁹² *Id.*

⁹³ *Id.*

⁹⁴ *Id.*

1. Third-Party Services and Compliance Risk

Third-parties can pose a significant risk to financial institutions when the vendors and their operations are not appropriately managed.⁹⁵ This is particularly true in the realm of BSA/AML compliance, where third-parties bear the burdens of monitoring the customers they service on behalf of financial institutions for money laundering or sanctions compliance.⁹⁶ In fact, the OCC identified the compliance risk challenges that banks face in managing third-party relationships, particularly as they pertain to third-parties performing Bank Secrecy Act functions.⁹⁷ The OCC also recognized that the risks associated with third-party relationships are compounded, or layered, as competition in a low interest rate environment drives financial institutions to adopt and expand product offerings or consumer bases, which often involves expanded reliance on third-parties.⁹⁸ This is certainly a risk profile that applies to indirect lending, as increased competition for auto loans has spurred large financial institutions and credit unions to develop new relationships with automobile dealers to increase the number of indirect auto loans generated. Indirect auto lending does not just rely on third-party relationships; third-party relationships are the essence of indirect lending, where the financial institution would be potentially unable to develop a client relationship and extend credit without the direct and active participation of the auto dealer in the product lifecycle.

⁹⁵ *Bank Vendor Management-The Next Compliance Frontier*, CCG CATALYST (June 25, 2014), <https://www.ccg-catalyst.com/bank-vendor-management-the-next-compliance-frontier/>.

⁹⁶ *Id.* (noting the compliance risks vendors pose to financial institutions).

⁹⁷ OFFICE OF THE COMPTROLLER OF THE CURRENCY, SEMIANNUAL RISK PERSPECTIVE 5 (Fall 2015) (“Regulatory amendments and reliance on third parties continue to create challenges for bank consumer compliance functions. Bank Secrecy Act (BSA) risk also continues to increase as criminal behaviors evolve and criminals leverage technology innovations”).

⁹⁸ *Id.* at 7.

a. *Applying the Lessons from Vendor Management to Non-Vendor Third-Party Relationships*

Some of the most important, and effective, portions of a BSA/AML compliance program center on client due diligence. In fact, broad KYC requirements include: (1) the collection of CIP, (2) CDD that includes customer risk rating, and (3) if necessary, EDD.⁹⁹ Using the definition of “customer” provided by the regulation, however, makes it seem as if the financial institution’s duty to perform due diligence should be limited to the person or entity opening the account.¹⁰⁰ However, as the amount of indirect auto loans and the importance of dealers operations continue to drive revenue growth at banks, the quality of relationships between financial institutions and dealers has become a source of operational, reputational, and regulatory risk point.¹⁰¹ As a result, financial institutions that work with third-parties to originate loans funded by the financial institution must ensure that it scopes the dealers into their BSA/AML due diligence compliance program. Though due diligence is generally a required category of KYC and dealers are not the lender’s customers, in order to ensure the integrity of the loans being originated and that financial crimes compliance obligations are met, it is important that financial institutions vet dealers as if they were customers.

While one of the primary focuses of KYC is the creation of a CIP, the primary focus of due diligence efforts for dealers is not so much on identifying the particular dealer, but of ensuring that the dealers origi-

⁹⁹ CCH INC., BAND COMPLIANCE GUIDE § 2010.11, 2017 WL 1655934 (Jan. 2017).

¹⁰⁰ 31 C.F.R. § 1020.100(c) (2017) (defining “customer” as: “(i) A person that opens a new account; and (ii) An individual who opens a new account for: (A) An individual who lacks legal capacity, such as a minor; or (B) An entity that is not a legal person, such as a civic club”).

¹⁰¹ Liz Furman, *Indirect Lending Grows Direct Impact on Credit Unions*, CREDIT UNION TIMES (July 10, 2016), <http://www.cutimes.com/2016/07/10/indirect-lending-grows-direct-impact-on-credit-uni> (noting that the quality of the dealer-financial institution relationship has continued to be a source of importance and concern as the auto lending portion of credit unions continues to grow).

nate loans in a way that does not pose significant ML/TF risks to the financial institution. This type of *channel due diligence*, named for the focus on the origination channel, in this case, dealers, should include advanced controls to vet dealers. This may include internal requirements that only approved dealers can originate loans and be funded, collection of beneficial ownership information from dealer owners, advanced credit/negative news checks and site visits of dealerships, and regular audits of the dealer's operations. The goal of a channel due diligence program is to ensure that the financial institution has a reasonable belief that the third-party which originates loans is originating loans which pose minimal ML/TF risk to the lender, or, if such assurance cannot be granted, that the financial knows so that it can create additional controls on loans originated by that dealer. In addition, a successful channel due diligence program aimed at dealer identification and risk-rating should be accompanied by clear instructions for enhanced due diligence or monitoring at increased intervals, much as a successful CDD program would for customers.

This type of strict oversight over third-parties has already been advocated for and is currently enforced by the OCC.¹⁰² While origination channel oversight is oversight of a third-party, the relationship cannot reasonably be categorized as a vendor relationship. However, recent OCC guidance to financial institutions on managing vendor risk is also valid for insight on how to handle channel due diligence. For example, the OCC's Supplemental Examination Procedures for Third-Party Relationships contains a number of testing/audit points that if met, would point to appropriate risk management of third-party relationships.¹⁰³ These Examination Procedures place emphasis on the quality of enter-

¹⁰² Gregory J. Millman, *Banks Grapple with Outsourcing Risk After OCC Guidance*, WALL STREET JOURNAL (Mar. 20, 2014), <http://blogs.wsj.com/riskandcompliance/2014/03/20/banks-grapple-with-outsourcing-risk-after-occ-guidance/> (noting that OCC guidance on vendor risk management was strengthened and tightened in 2014).

¹⁰³ OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULLETIN 2017-7: THIRD-PARTY RELATIONSHIPS SUMMARY (Jan. 24, 2017) (establishing supplemental examination procedures for use during regulatory review of a financial institution's vendor management program).

prise policies,¹⁰⁴ on-going monitoring of the third-party's activities,¹⁰⁵ and internal risk assessment systems to monitor third-party risk.¹⁰⁶ All three of these program elements, while not exhaustive, are presumably steps all federally chartered banks have taken already and only need to be repurposed (to account for ML/TF concerns) to form the backbone of channel due diligence for third-party originated loans. It is also important to remember that third-party vendor relationship guidance issued by the OCC is, like BSA/AML guidance, risk-based, which gives financial institutions the ability to design flexible CDD/EDD programs for dealers based on the potential compliance/regulatory/legal risks they pose.¹⁰⁷

b. Third-Party Relationships with Unregulated Fintechs

In the world of indirect lending, or *brokered retail lending*, as this article prefers to call this type of business operations, fintechs play an important role.¹⁰⁸ Not only do fintechs serve as loan originators, bringing the customers to the lenders, whether by connecting dealers to lenders or via consumer-facing portals, they also serve as conduits for fund disbursements. It is important to recognize the two primary roles fintechs play, as each relationship carries nuances to the compliance regimes that banks should enact.

The first type of fintechs relationship mentioned above is that relating to client/customer origination. As this article has previously

¹⁰⁴ *Id.* at 9.

¹⁰⁵ *Id.* at 14 (on-going monitoring includes collection of, and updates to, previous due diligence efforts to ensure the financial institution has a proper understanding of the third-party's financial condition, compliance burdens and programs, and business practices that may pose a risk to the financial institution).

¹⁰⁶ *Id.* at 17.

¹⁰⁷ Paul Schaus, *When Vendor Risk Management Goes Too Far*, AM. BANKER (Aug. 28, 2014), <https://www.americanbanker.com/opinion/when-vendor-risk-management-goes-too-far> (noting that the OCC's guidance for vendor management by banks is risk-based).

¹⁰⁸ Miller, *supra* note 70.

mentioned, there are two prominent fintechs in this space, DealerTrack and Route One, both of which connect auto dealers with lenders/financial institutions.¹⁰⁹ It is important to understand that the dealer inputs the customer's information into the applications, which identify, based on pre-determined criteria, potential lending opportunities for the dealer's customers. Given the origination functions performed by these fintechs, it is important to appropriately frame the financial institution's compliance burdens with the scope of the vendor's responsibilities. Of paramount importance for the lender, if they are not independently collecting and verifying information during underwriting, is the notification¹¹⁰ and collection of information confirming the customer's identity.¹¹¹ Since a third-party fintech, or potentially the dealer, is providing notification of the collection of information under CIP, it is important that the division of responsibilities be fully understood by all parties involved, duplicate processes on behalf of the lending institution be created, and that responsibilities are memorialized by contract and internal procedures. This can be a particularly difficult control environment to establish and regulate because many financial institutions that rely on digital loan origination have established customer portals/applications that rely on "hard stops" in the application process if relevant (i.e. legally required) information is not input. A lender that relies on fintechs for client origination may not have the appropriate level of oversight to dictate what information needs to be collected or ensure that technological controls such as a "hard stop" are put in place, monitored, and tested. This concern is amplified in the world of fintechs, where there is little regulatory oversight, particularly as it pertains to BSA/AML obligations. Additionally, since KYC requires the risk rating of customers, it is important that the financial institution either be able to contractually rely on risk-rating performed by intermediary third-parties (if those risk-ratings account for potential BSA/AML concerns) or perform risk-rating be-

¹⁰⁹ *Id.*

¹¹⁰ 31 C.F.R. § 1020.220(a)(5)(i) (2017) (requiring adequate notice to customers that information is being collected to verify the customer's identity).

¹¹¹ 31 C.F.R. § 1020.220(a)(2)(i) (2017).

fore, or immediately after, client onboarding.¹¹² Financial institutions who identify potentially high-risk customers must also be able to timely execute enhanced due diligence to collect information from the borrower, a feat that is complicated by the fact that a third-party both has controlled and may continue to control the client relationship.

A second type of relationship on which financial institutions may rely is the fintech refinancing relationship. In this case, the loans are likely requested by consumers, exclusively through digital channels, and the fintech is not only responsible for fulfilling KYC responsibilities, but may also be facilitating the disbursement of funds. Such a relationship is common in refinancing, where consumers with pre-existing auto loans make a request through an application like OpenRoad, which connects the borrower to potential lenders, much as an application like DealerTrack would.¹¹³ However, the lender, who then completes their own underwriting, would disburse funds to the fintech, which is then responsible for funding the re-finance and paying off the original lender. This is a commonly misunderstood relationship that needs substantial clarification. First, it is paramount to determine which party is the client in a fintech originated refinance. A customer, as defined by the statute, is a person who opens a new account, whether for that individual, or someone who lacks capacity or for an entity that is not a legal person.¹¹⁴ According to the statutory definition, an account is a “formal banking or business relationship”, whether provided in the form of an actual account, an extension of credit, or a deposit box, or cash management service.¹¹⁵ In the case of fintech originated refinance, the borrower is seeking an extension of credit for which they will be responsible to repay. The question then becomes: Which party is responsible for accepting repayment? If the customer pays the fintech directly during the maturity

¹¹² CCH INC., BAND COMPLIANCE GUIDE § 2010.11, 2017 WL 1655934 (Jan. 2017).

¹¹³ Miller, *supra* note 70.

¹¹⁴ 31 C.F.R. § 1020.100(c)(1) (2017).

¹¹⁵ 31 C.F.R. § 1020.100(a)(1) (2017).

of the loan and the fintech makes payments to the lender to pay down the refinance payment issued by the lender to the fintech, it would appear that the fintech is the lender's customer, while the borrower would be the customer of the fintech. However, usually the customer would remit payments directly to the bank for the extension of credit and the fintech would serve only as an intermediary. If there were to be a default, the financial institution would look to the retail borrower, not the fintech, for compensation. This is reflected by the fact that either the fintech and/or the lender perform credit underwriting on the retail borrower. Given this arrangement, the financial institution is responsible for all aspects of the CIP, including notification, collection, and verification of identity information from the retail borrower, as well as risk-rating and EDD, if necessary. Additionally, as long as the financial institution is receiving payments from the retail borrower, it is responsible for customer information refresh responsibilities, transaction monitoring, and regulatory reporting.

While the fintech originated refinance in which the customer makes payments to the financial institution still retains the retail-borrower-as-customer lending format and subsequent BSA/AML responsibilities, it would seem odd to completely release the financial institution from having any BSA/AML responsibilities as they pertain to the fintech. This is because it seems that fintechs may also be clients of the financial institution. If a customer is one who receives formal banking services, wouldn't the fintech that receives a lump-sum funds disbursement be considered a recipient of formal banking services? Although it may not be an account, credit, or trust relationship, this is more than a vendor relationship (there are no services being provided to the financial institution) and thus should be regarded with a greater level of AML scrutiny. In fact, the refinancing fintech's business model requires the extension of funds by the financial institution to the fintech for the fintech to successfully refinance a consumer's loan. Viewing the extension of services in this light, it appears as if financial institutions should consider these refinancing fintechs customers, in the BSA/AML compliance sense, or at least something more significant than vendors subject to basic OCC due diligence requirements. Even recognizing them as financial intermediaries and subjecting them to CDD (including risk-rating/EDD, sanctions screening, and transaction monitoring) should be

considered necessary in the course of any prudent AML/CFT compliance program.

IV. CONCLUSION

Business models utilizing indirect lending, particularly those related to automobile and recreational vehicle financing are a growing source of revenue among a number of different types of financial institutions. Since this is a typical finance product offered by large and small banks alike, it is important that the funding institution build a robust, yet risk-based BSA/AML compliance program that mitigates potential money laundering and terrorist financing risks. This is especially important as automobile and recreational vehicle sales can be attractive targets for both types of illicit financing. However, the structure of indirect lending can present a number of challenges for financial crimes professionals and regulators alike with confusion over applicable program elements and compliance obligations that are required during the life-cycle of an indirect loan. These challenges are multiplied by the reliance on third-party relationships; often times with under-regulated fintechs or with parties with whom the financial institutions has failed to establish adequate third-party oversight. Even labeling this type of financing *indirect lending* contributes to the confusion, as it allows banking professionals to separate the client from the intermediary, which obfuscates the need for comprehensive controls and oversight over the intermediary. In fact, a more appropriate term for this type of lending might be *brokered retail financing*. Recognizing the importance of the originating intermediary to the soundness of the financial crimes compliance program is a prerequisite for financial institutions to craft risk-based, yet robust, AML/CFT compliance programs.