Financial crime: Why are securities markets vulnerable?

Received (in revised form): 16th June, 2021

Jonathan Ehrenfeld
Strategy Director, SWIFT, Belgium

Jonathan Ehrenfeld

Jonathan Ehrenfeld *is Strategy Director at SWIFT and is responsible for securities strategy. He is a key contributor to a number of different industry working groups, including the International Securities Services Association (ISSA). Before joining SWIFT in 2011, he was an assistant professor at the University of Brussels.*

ABSTRACT

In the last five years, regulators have begun to focus on compliance and money laundering risks specific to securities markets. It is clear to them that the ways in which securities are issued, traded, cleared and settled create a series of opportunities for criminals and that these opportunities make the securities industry vulnerable to financial crime. This paper explains where the vulnerabilities lie in securities markets, explores the regulatory and financial consequences for individual firms of failing to address these vulnerabilities, identifies guides to action and obstacles to effective compliance and discusses how they can be overcome at affordable cost.

Keywords: securities, due diligence, AML, compliance, capital markets, ISSA, FATF

Avenue Adèle 1,
1310 La Hulpe,
Belgium
Tel +32 655 36 69;
E-mail: jonathan.ehrenfeld@swift.com

Journal of Securities Operations & Custody
Vol. 13, No. 4, pp. 346–353

BACKGROUND

Anti-money laundering (AML) measures date back 50 years and efforts to counter the financing of terrorism (CFT) started nearly 20 years ago. Although securities markets were always recognised as being at risk, until recently regulators concentrated on cash payments, where the opportunities to commit financial crime are more obvious. In the last five years, regulators have begun to focus intently on the AML and CFT risks specific to securities markets. Initially, regulatory concern centred on the use of securities to launder illicit cash but as AML and CFT programmes have tightened controls in cash payments, regulators believe securities markets have become a more tempting target for criminals and terrorists. The high values and volumes of transactions in the capital markets, the range of products available and the high levels of intermediation in securities transactions, in particular, provide many tempting targets for money launderers and terrorists.

VULNERABILITIES OF THE SECURITIES MARKETS

Securities markets provide a host of tempting targets. They transact in high value, which makes securities transactions in particular attractive for laundering large sums of money; they trade in high volumes and settle quickly, leaving market participants with little time to identify and prevent criminal activities hidden in daily flows that are measured in the billions. Securities markets transactions also contain many more points of vulnerability than a straightforward cash payment between two bank accounts. Clearing and settlement, corporate action notifications and instructions, dividend payments, redemptions, securities on loan and margin calls are all open to being falsified in order to transform the proceeds of crime into legitimate cash or transfer value to terrorists. The extended

chains of intermediation in securities transactions create further opportunities for crime: a typical equity transaction might entail the exchange of valuable information between a dozen intermediaries, any one of which can be compromised and potentially expose counterparts to loss or theft. The array of services provided is equally wide. It includes issuance, research, portfolio management, trade execution, trading, clearing and settlement, underwriting, private placement, fund distribution, fund accounting, transfer agency, order routing, mergers and acquisitions, securities lending and financing, collateral management and clearing of exchange-traded and over-the-counter (OTC) derivatives. All of these activities present discrete AML and CFT risks. Furthermore, reliance on third parties for technology, such as execution and order management; information about settlement details, such as standing settlement instructions (SSIs) and bank identification codes (BICs); asset prices, such as stock market values, is high, and increases the risk of information being manipulated.

In summary, the wide varieties of information exchanged between intermediaries in securities markets create multiple points of entry for money launderers and criminals. Uniquely among financial markets, securities markets also create opportunities for criminals to generate funds illicitly as well as launder or transfer them, through insider trading, market manipulation and fraud.

Despite these vulnerabilities, the securities industry has yet to experience a major reputational setback of the kind experienced by numerous banks in their cash management and payments businesses. This has prompted concern among regulators, especially in the United States, that the securities industry is not taking its obligation to counter money laundering and terrorist financing seriously. As a result, regulators are increasing the pressure on the securities industry to improve its performance creating a serious regulatory and compliance risk for securities firms. If they do not keep up with changes in laws and regulations in the jurisdictions where they operate, they will be liable to substantial financial penalties, exemplary fines and sanctions that exclude them from conducting certain businesses.

POINTS OF VULNERABILITY IN SECURITIES MARKETS

Physical securities. Most securities are dematerialised but bearer bonds and shares persist and are almost equivalent to cash in terms of the ease with which they can be transferred. It is easy to buy and sell them without the transaction being recorded or reported.

Low-priced securities. The most prevalent form of money laundering entails either acquiring companies that issue low value equity, or issuing shares to holders of illicit funds, or acquiring stock before a company goes public, or 'pump-and-dump' schemes in which false information is released to inflate the value of stock purchased with illicit funds prior to sale.

Private placements. Issuers can place securities with holders of illicit funds, or investors can use illicit funds to purchase privately placed securities. Usually, the issuer and the investors are closely connected.

Offshore funds. Offshore locations run AML checks on investors in funds domiciled in their jurisdiction but rely on information from third parties, which may be tainted.

Delivery free of payment. Most transactions are settled by delivery against payment (DvP), but securities are still sometimes delivered free of payment. This creates opportunities to steal securities without paying for them or generate bogus instructions to deliver securities to a fake account.

OTC options. Criminals structure contracts which guarantee one party will receive a payment based on the difference between the strike and market price. With

options contracts settling in cash rather than securities, illicit funds can be laundered.

Digital trading platforms. Off-exchange trading allows investors to buy and sell securities without going through a regulated intermediary such as a broker or a bank. Trading platforms can also allow investors to trade anonymously.

Innovative products. Many securities are issued and traded before they are regulated. Initial coin offerings (ICOs), which were not initially classified as securities, are a recent case in point. The regulatory treatment of crypto or tokenised assets remains uncertain in many jurisdictions.[1]

Complex products. Products which are difficult to value, due to their illiquidity or bespoke nature, create opportunities for sophisticated criminals to exploit the lack of a market price.

Reliance on representations. Intermediaries in the securities markets rely on other intermediaries to conduct proper due diligence on their customers, including sources of funds. There is no single link in a securities intermediation chain with complete oversight of a transaction.

Nominee and omnibus accounts. Nominee accounts create opportunities to obscure beneficial ownership by using a corporate name. Omnibus accounts, in which assets belonging to multiple clients are commingled, also conceal beneficial ownership. Both make it harder to identify criminals.

Reference data. Crucial reference data, such as SSIs, is reliant on manual updates which create opportunities to divert deliveries of cash and securities.

Reliance on third-party sources of data on individuals and states. Lists of politically exposed persons (PEPs) and sanctioned states and individuals come from a limited range of sources, making it hard to verify data, and increasing the risk of manipulation.

Cyberattacks. Phishing e-mails, ransomware and other methods are used to steal money or securities or manipulate records. The high-levels of intermediation in the securities industry means a compromised firm can affect its counterparts.

Centralisation of functions. Securities transactions are matched through centralised trade-matching services, cleared through central counterparty clearing houses (CCPs), settled in central securities depositories (CSDs) and reported to trade repositories (TRs). All of these market infrastructures concentrate the risks of theft, fraud and ransom.

Outsourcing and offshoring of functions. Securities markets firms have outsourced and offshored previously internal functions. Many operations are now performed by third parties, some based in low-cost countries with higher AML and CFT risk, where it is more difficult to run effective checks on rogue employees or contractors.

Predictability. Securities settle transactions and pay entitlements to pre-agreed timetables, making it easier for money launderers and terrorist groups to know when to attack a transfer of value.

Perverse incentives. Securities firms have a difficult balance to strike between individual incentives and internal controls which money launderers and terrorist financiers can disrupt.

Sanctioned states and individuals. Sanctions which deny states or individuals access to the global financial system can encourage sanctioned states and individuals to use illicit means instead, including abuse of the capital markets.

FOCUS ON CUSTOMER DUE DILIGENCE

There is growing evidence that the aforementioned vulnerabilities are being exploited. Over the last seven years, the Financial Industry Regulatory Authority (FINRA) in the United States has levied many fines on securities markets firms amounting in total to more

than US$100m.[2] More than half the enforcement cases entailed money being laundered by criminals investing in securities issued by businesses they controlled. Importantly, fines of this kind are often accompanied by sanctions against individuals. Recent penalties levied by FINRA singled out individual compliance officers at individual firms for suspension, or fines, or both, for shortcomings in the fulfilment of corporate financial crime compliance obligations. Singling out individuals also encourages the development of a stronger culture of compliance which ultimately rests on three basic disciplines: transaction monitoring, sanctions screening and effective customer due diligence (CDD).

CDD requires securities firms to identify the beneficial owners of legal entity customers, understand the nature and purpose of customer accounts, conduct ongoing monitoring of customer accounts to identify and report suspicious transactions, and update customer information.[3] Recent focus on CDD requirements marks a decisive change in regulatory attitudes towards AML and CFT compliance. Transparency into the ultimate ownership of financial assets was always a crucial component of financial crime compliance, but AML originated in the monitoring of financial transactions and holdings rather than the identity of the ultimate customer, and CFT initially followed the same pattern. The introduction of stricter CDD rules is also symptomatic of a shift in the emphasis of AML and CFT from transactional analysis to know your customer (KYC) — who they are, where their funds come from, why they are active in the market and whether the firm should be doing business with them — as the principal source of risk. For the securities industry, in which high-levels of intermediation create a natural reliance on assurances from the previous link in the transaction chain, KYC and know your customer's customer (KYCC) represent a radical change in regulatory expectations. In complying with CDD requirements, however, securities markets firms have to surmount one other major obstacle: the omnibus account. Although omnibus accounts are operationally efficient, they commingle the assets of many customers and counterparts. In theory, this complicates the task of establishing the identity of the ultimate beneficiary of a transaction or holding. The industry has traditionally solved this problem by relying on assurances from the previous link in the transaction chain that their client is not a money launderer or terrorist or sanctioned person. At the same time, industry practitioners are certain that the risks that omnibus accounts will be used to launder money or transfer resources to terrorist groups do not warrant the sacrifice of an account structure which has proved its worth in terms of scalability and low cost. Its confidence is based on increased CDD throughout the securities chain, and firms have responded to the regulatory pressure on omnibus accounts with practical measures that offer sufficient transparency into beneficial ownership without losing its administrative convenience and economic benefits.

'The Financial Crime Compliance Principles for Securities Custody and Settlement' published by the International Securities Services Association (ISSA) aim to make these measures more effective by contractual means.[4] The securities services industry has a long tradition of transmitting legal and regulatory obligations across national borders by embodying them in contracts with counterparts. In this case, encouraging counterparts to meet the standards set by the ISSA principles eliminates the need for expensive KYCC checks where firms need to conduct due diligence on the customers of their customers. Instead, securities firms can issue the ISSA Financial Crime Compliance Sample Questionnaire (reference) to

their counterparts, which assesses whether their clients are subject to detailed AML and CFT checks and controls. It also asks what types of clients they have, to identify any that represent a high AML or CFT risk, and what types of account their assets are held in.[5] This aligns the ISSA principles with the risk-based approach of the Financial Action Task Force (FATF), whose 40 Recommendations of 2012, updated in 2018 have, through multiple subsequent revisions, become the de facto global standard for AML and CFT compliance.[6] In fact, while the 40 FATF Recommendations are directed at national governments rather than securities market practitioners and most of them concern legal issues (such as making money laundering and terrorist financing criminal offences or granting immunity to whistle-blowers) or commercial activities (such as casinos and dealers in precious stones and metals) that are not within the span of control of securities firms, the most important subset of recommendations, mostly to do with the prevention of money laundering and terrorist financing, have a strong correspondence with the ISSA principles in terms of intent if not of detail. Similarities between the ISSA principles and the FATF recommendations can be found on the measure to mitigate AML and CFT risks, on the best practices when conducting CDD, on implementing provider, correspondent or counterparty checks, on the safe reliance in third parties or intermediaries, on the importance of focusing on high-risk countries and on increasing the transparency of beneficial ownership of securities, among others.

OVERCOMING DIFFERENCES BETWEEN NATIONAL REGULATORY REGIMES

Unlike the ISSA principles, which aim to provide practical advice to market participants, the FATF recommendations are aimed not at industry practitioners but at regulators and governments expected to implement them as national law. They have been endorsed by the International Monetary Fund (IMF) and the World Bank, and by more than 180 nation-states. Endorsement mitigates the risk of being blacklisted because any state which does not require regulated firms to follow the FATF recommendations can expect to appear on blacklists issued by the European Commission as well as FATF. As blacklisting makes it difficult for financial institutions to gain access to global financial markets, almost all jurisdictions support the FATF recommendations. In theory, this means that the AML and CFT rules in most jurisdictions are equivalent. In practice, local implementations are not the same. By providing practical guidance, enforced by bilateral contracts, the ISSA principles provide a flexible means of overcoming these differences. The ISSA conviction is that the key to an effective AML and CFT regime is making sure that customers are performing to the right standard. It is not alone in this conviction. The Association for Financial Markets in Europe (AFME) has published a Post Trade Due Diligence Questionnaire for banks to issue to their intermediaries and for many years — it includes questions about AML and CFT[7] — and the Wolfsberg Group has issued a Correspondent Banking Due Diligence Questionnaire which has sections on AML and CFT as well.[8] Similar developments have taken place in other industries including trade finance since 2011.

THE SCALE OF THE FINANCIAL CRIME COMPLIANCE CHALLENGE

Nevertheless, achieving compliance with the multiple laws and regulations governing financial crime represents a substantial challenge in terms of information capture, processing, analysis and decision-taking.

The costs of meeting the challenge are significant. But paying them matters, because financial institutions are already being fined by regulators not for financial crime per se but for shortcomings in AML and CFT systems and controls. A potential solution to these difficulties lies in the adoption of new forms of risk-based surveillance technology. Rules-based techniques, which have tended to produce unmanageably large numbers of false positives, are being surpassed by the application of artificial intelligence (AI) and machine learning (ML) capable of sifting at speed through the structured and unstructured data about transactions, portfolio holdings, counterparts and customers. But these technologies can be too expensive for smaller firms, creating a risk that financial criminals will focus their attention on securities houses less able to protect themselves. Because of that, technology vendors should focus on a range of services that are especially valuable to smaller firms with limited compliance budgets. Industry utilities can also offer mutualised solutions to reduce the cost for all firms in order to do name or entity screening (which vets the names of individuals, corporations and other entities against lists of PEPs, their relatives and associates, and sanctioned individuals, organisations and states), sanctions screening (allowing firms to screen payments and securities transactions against lists of sanctioned states, such as those provided by the Office of Foreign Assets Control (OFAC) and the European Union (EU)) or to share KYC datasets (such as those proposed by the Wolfsberg Group for correspondent banking or ISSA for securities and custody networks).

In any case, larger firms will also struggle to extract the full benefit of the new technologies unless they can overcome the silos that currently make it impossible for them to understand the full range of interactions that any of their clients can have with different parts of their own organisation. Yet a great deal of data about customers and shareholders is available to securities firms: screening W-8BEN withholding tax exemption forms submitted to the Internal Revenue Service (IRS)[9] in the United States, for example, would reveal the domicile of the investor who owns the security; screening corporate actions instructions, where investors are obliged to disclose themselves, would also reveal the identities of beneficial owners; and finally since September 2020, the Shareholder Rights Directive II (SRD II) gives issuers registered in the EU the right to identify their shareholders, requiring intermediaries to cooperate in the identification process. All of these datasets can then be checked against lists of PEPs supplied by firms such as Dow Jones.

Given the opportunities to launder money through the issuance of (often low priced) securities or the private placement of securities, reading what is disclosed in the prospectus or information memorandum for the issue is a useful AML and CFT discipline. It is more difficult to read documents, because the information in them is unstructured, but today machines are improving their ability to read and detect useful clues in natural language texts. Nevertheless, in the absence of cost-sharing schemes devised by vendors, or the establishment of AML and CFT surveillance utilities, the securities industry needs to find effective and affordable means of detecting and preventing financial crimes and averting potential financial crime compliance breaches. In recent years, SWIFT has cocreated with its community a range of shared utilities that firms can use to fulfil their AML and CFT compliance obligations without incurring heavy additional costs as most of the cross-border payment transactions where AML and CFT risk are acute are in fact carried on by the SWIFT network today. Furthermore, according to

an analysis of SWIFT traffic,[10] at least 30 per cent of international payments messages were originated or exchanged with a securities counterparty as result of a securities-related process (trade, corporate actions, funds, collateral management). In 2020, the SWIFT securities community also pushed for the extension of the global payments innovation (gpi), which enables financial institutions to share the details of payments transactions with each other, to these cash movements related to securities transactions. The increased transparency into the status of payments en route to beneficiaries or final accounts, the fact that each payment is tagged with a unique end-to-end tracking identifier (UETR) that enables all parties to the payment to recognise it and the ability to stop and recall a payment, will make it harder for criminals to launder money through the securities markets.

The securities industry, however, faces mounting AML and CFT risks. These are most obvious in the cash legs of securities transactions but every aspect of the securities industry, including issuance, trading, safekeeping and settlement, presents opportunities for money to be stolen or laundered. If securities firms are to avoid the reputational and financial costs of AML and CFT compliance failures, they need to develop a culture of compliance. That culture should be based on adherence to official and industry guidance on how to manage AML and CFT risks. It should be implemented by a commitment to the basic disciplines of screening transactions and performing effective due diligence on customers and counterparts, and by making full use of the many and varied financial crime compliance services that are already available. Inevitably, it will take time for vendors or the industry as a whole to develop and agree upon mutualised surveillance technology and services of this kind. Equivalent products and services are well developed in cash payments and securities trading, but the increased regulatory interest in post-trade securities markets as a source of AML and CFT risk is of relatively recent origin. This means that it is equally recently that financial crime compliance specialists identified post-trade services in the securities industry as an opportunity.

References

(1) Financial Action Task Force – FATF (2019) 'International Standards on combating money laundering and the financing of terrorism and proliferation: the FATF recommendations', available at: https://www.fatf-gafi.org (accessed February 2021).

(2) FINRA (2021) 'Anti-money laundering news releases', available at: https://www.finra.org/media-center/newsreleases (accessed February 2021).

(3) Financial Crimes Enforcement Network – FinCEN (2018) 'Customer due diligence requirements for financial institutions', available at: https://www.federalregister.gov (accessed March 2021).

(4) ISSA (2019) 'Financial crime compliance principles for securities custody and settlement', available at: http://www.issanet.org (accessed February 2021).

(5) ISSA (2019) 'Financial Crime Compliance Questionnaire – ISSA DDQ', available at: https://www.issanet.org (accessed March 2021).

(6) FATF (2018) 'Risk-based approach guidance for the securities sector', available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-securities-sector.html (accessed February 2021).

(7) AFME (2021) 'Due Diligence Questionnaire', available at: https://www.afme.eu/Divisions-and-committees/Post-Trade/AFME-Due-Diligence-Questionaire-2021 (accessed March 2021).

(8) The Wolfsberg Group (2020) 'Correspondent Banking Due Diligence Questionnaire', available at: https://www.

wolfsberg-principles.com/wolfsbergcb (accessed February 2021).
(9) IRS (2020) 'W-8 BEN certificate of foreign status of beneficial owner for United States tax withholding and reporting', available at: https://www.irs.gov/forms-pubs/about-form-w-8-ben (accessed March 2021).
(10) SWIFT (2021) 'Traffic volumes of MT 103 and MT 202 sent and received linked to securities-related activities', available at: swift.com/BI (accessed February 2021).