Europe's Banks Must Step Up To Crack Down On Financial Crime

April 18, 2019

Key Takeaways

- We see reducing tolerance from investors, clients, and regulators for banks making missteps in the area of financial crime risk.
- European banks have reduced their inherent financial risk profiles, but we expect many will review their governance of this area and step up investments in smart technologies and data analysis techniques.
- We continue to take a differentiated approach when concerns arise. This reflects the varying fact pattern and gravity of each case, and so the varying financial and franchise implications for the affected banks.

PRIMARY CREDIT ANALYST

Giles Edwards
London
(44) 20-7176-7014
giles.edwards
@spglobal.com

SECONDARY CONTACTS

Bernd Ackermann
Frankfurt
(49) 69-33-999-153
bernd.ackermann
@spglobal.com

Letizia Conversano
Dublin
353 1 568 0615
letizia.conversano
@spglobal.com

Emmanuel F Volland
Paris
(33) 1-4420-6696
emmanuel.volland
@spglobal.com

Salla von Steinaecker
Frankfurt
(49) 69-33-999-164
salla.vonsteinaecker
@spglobal.com

Cihan Duran
Frankfurt
(49) 69-33-999-242
cihan.duran
@spglobal.com

See complete contact list at end of article.

Six months ago, we examined the checkered track record of the European banking sector on the topic of anti-money laundering (AML) and sanctions compliance. While financial crime is a key operational risk for banks globally, we noted that European banks appear to be over-represented in the steady flow of cases of banks censured for AML and sanction breaches. We saw some signs of progress at the bank-specific, member state, and regional levels, but there seemed to be few reasons to be optimistic that such problems would not recur in Europe, in the medium term at least (see "Déjà Vu All Over Again: Money-Laundering And Sanctions Woes Continue To Haunt Europe's Banks").

Six months on, European banks continue to suffer from a steady drip of troubling news. Further details and allegations related to the various Laundromat scandals continue to emerge, with Swedbank now under the spotlight having fired its CEO, after which the Chairman stood aside. ING and Deutsche Bank continue to feel the ire of regulators as they work to enhance customer due diligence. Standard Chartered has now finally exited its 2012 deferred prosecution agreement, after more than six years and well over $2 billion (in settlements and remediation costs). Unicredit agreed to pay $1.3 billion to U.S. authorities to settle claims of sanctions breaches during the 2002-2011 period. UBS has appealed the guilty verdict of its tax prosecution in France, having previously settled tax-related cases in the U.S. and Germany. And these are just the most recent examples.

Typically, these allegations relate to legacy events, often dating from the 2007-2015 period. But such problems can take a while to emerge. So what comfort should investors have that in the

coming one to two years they will not see emerging problems that stem from today's activities? Arguably, only a little. The latent risk has been reduced by banks' widespread enhancements to customer due diligence and tax attestations and related offboarding of noncompliant clients, as well as improved tax transparency. However, some banks will also need to change their governance of this risk to take a rather more holistic approach, and to invest in new technology and data analysis techniques. This would be an act of enlightened self-interest in two respects:

- Financial crime is a hard-to-quantify nonfinancial risk that can have significant adverse consequences for a bank; and
- Compliance costs have risen steadily across the industry, but investments could yield significant efficiencies as well as improve effectiveness.

The banks cannot do it alone, however. For the fight against financial crime to be truly effective, this will likely require changes to financial regulation, data and company law, greater investigatory resources, and efforts to remove technical obstacles.

The Consequences Of Financial Crime Risk Failures Are Rising

Financial crime control failings are hardly a new phenomenon in the financial services industry, but the transparency of alleged transgression appears to be rising thanks to the efforts of investigative organizations, leaks from bank insiders, regulators' greater willingness to reprimand banks publicly, and the rapid and widespread sharing of information via social media. It is notable, though, that the banks currently under the spotlight hail from countries that are among the most liberal in the world with a free and active press (for example, Sweden, Denmark, The Netherlands, and Germany). In other countries, such cases may not have been revealed, though this does not mean they do not exist.

The negative reaction that surrounds such cases is not new, and it may well remain transitory in some lesser cases, for example where the identified problems are historic and contained, and the associated costs are modest. But this reaction is growing, in our view, for several reasons:

- Increased investor interest and concern about environmental, social, and governance (ESG) risks in investee companies;
- Increased regulatory willingness to flex muscles so increasing the costs (in management time and money) of transgressions;
- Reduced reputational risk tolerance among customers sensitized to ESG risks; and
- The continued relatively benign environment that currently pushes traditional credit and market risks to the background and other risks forward.

In short, while the market remains typically forgiving of transgressions, the franchise and solvency risks associated with financial crime blow-ups are increasing, in our view. In extremis, and as the closures of few small banks in the Baltics, Malta, and elsewhere show, a business model can quickly become nonviable if clients, counterparts, service providers, and ultimately regulators lose confidence in the bank. Unlike for credit risk, when it comes to financial crime risk, a business model based on servicing clients that other banks will not touch is not a business model.

S&P Global Ratings does not overlook that the ultra-benign credit environment will start to normalize, and market volatility seems to occur in ever more frequent spasms rather than being predictably unpredictable. However, we see hard-to-measure nonfinancial risks, like financial crime and cyber, as key, ongoing issues for European banks. We note the same concern among

many of the banks' senior management teams and risk officers. And yet, we suspect that management teams at some banks sometimes struggle in these areas:

- Defining financial crime risk appetite;
- Making this risk a central factor in deciding how, where, and with whom they do business;
- Moving beyond a box-ticking approach to financial crime compliance by enabling their capabilities to use their multiplicity of data sources intelligently; and
- Truly embedding financial crime compliance as a key responsibility of staff wherever they are in the bank. Cyber risk is not just an IT responsibility, and financial crime risk is by no means just a compliance responsibility.

Financial Crime Can Happen Anywhere

A disproportionate number of large Nordic banks are currently the subject of allegations around financial crime concerns: most visibly Danske and Swedbank, but also SEB and Nordea. While many European banks wrestled with a variety of sustained challenges over the past decade, investors perceived these banks as among the most trusted and well-managed in Europe. Many of them pursued logical extension growth strategies in neighbouring Baltic countries, but ultimately these jurisdictions have proven to be a key, though by no means the only, conduit for dirty money that finds its way into the European banking system.

Undoubtedly, some jurisdictions pose a higher risk than others. But the real problem is that these banks are not alone in being criticized and financial crime can arise anywhere, because of the high level of interconnectedness of financial systems and the continuing evolution of techniques to launder money by criminal organizations/third-party money launderers. Many of the companies involved in the various identified Laundromat cases are domiciled far from the original locations of the funds: in offshore centers, but also in key European financial centers, such as the U.K., particularly when they allow opaque beneficial ownership structures.

Tighter Bank Risk Appetites Could Affect Higher-Risk Jurisdictions And Cross-Border Payment Activities

For all the alleged problems of the Nordic banks in the Baltics, it must surely be possible to deliver well-controlled, compliant, banking services in these countries for residents and non-residents alike. However, the problem for markets that are perceived to be at higher risk from financial crime is that overseas banks may conclude that the costs of operating in those jurisdictions or interacting with domiciled counterparts outweigh the benefits. More generally, this could also be true for banking activities, such as remittances and other international payments when the counterparts and fund origins are hard or impossible to source. Internationally-active banks have cut back their higher risk correspondent relationships and, on occasion, exited certain markets due to an unacceptable risk profile. And these markets often do not offer large or deep revenue pools. Therefore, without remediation in local standards, these jurisdictions risk a marked reduction in credit supply or becoming a financial island, cut off from some of the normal channels for international payments.

Rising Expectations For Banks' Risk Controls

Against this backdrop, it is probably unrealistic to expect banks to spot every fraudulent or illegal transaction or nefarious client. While one could consider this as a desirable outcome, this is not what banks are asked to do, and it is not what they can do, unless they vastly increase resources, and customers and regulators settle for a degraded and more expensive service proposition. For sure, banks expose themselves to legal risk if they become the inadvertent conduit for any financial crime. But beyond establishing minimum standards on customer due diligence, the law requires that banks adopt a risk-based, diligent approach to addressing financial crime risks. Standing still will not be sufficient, however. Minimum customer due diligence standards continue to rise. We anticipate also that banks' greater use of technology (notably machine learning) and data aggregation will improve the sophistication, effectiveness, and efficiency of their control frameworks, if implemented correctly.

More importantly though, we look for a step-change in governance and mindset across the industry. In the Danske case, for example, it appears that internal reports or whistleblowing warned top management that there was something wrong, but these seemingly did not invoke a sharp reaction. It is easy to judge missteps with the benefit of hindsight, but, for example, any management team might need to think critically about why it generates super-profits in some locations or activities. Furthermore, the EU Whistleblower Protection Directive, approved by the European Parliament earlier this week, toughens requirements on banks (and other corporate entities) to follow up on whistleblowing reports and provide timely feedback to the whistleblower. It also provides clearer mechanisms for whistleblowers to report concerns to regulators or even publicly.

To defend their franchises, banks will need to move beyond achieving a minimum level of technical compliance, for example with due diligence documentation. It is not easy to develop a risk framework that adequately captures low-frequency, high severity non-financial risks. But bank Boards will need to find a way to exercise their broad mandate effectively, by establishing a clear risk appetite, demanding tools that allow them to track execution and challenge management, and driving through cultural change. Even when banks have a clear risk framework, the sophistication of the systems can heavily influence the effectiveness and efficiency of the delivery of those controls. We already see banks' different willingness and capacity to materially invest to upgrade incumbent systems supported by state-of-the-art technology (machine learning in combination with artificial intelligence).

As for cyber risk, when it comes to financial crime risk the nature of the threat continues to evolve and the system is arguably only as strong as its weakest part. We expect therefore that conduct regulators will pressure all banks to continue to invest and enhance their risk control frameworks. Furthermore, as the costs of non-compliance rise, prudential regulators could well take greater interest in a bank's exposure to, and management of, financial crime risk.

The Banks Cannot Do It Alone

Just as importantly, the authorities play a key role in addressing financial crime risk. Policymakers continue to tighten the regulations--most recently through the implementation of the EU's Fifth Anti-Money Laundering Directive. Increased global information sharing, for example the automatic exchange of tax-related information under the OECD's Common Reporting Standard, could improve detection rates and inhibit some criminal activity. But no matter how strong the supervision in one country, international cooperation between intelligence units and supervisors

remains key to identifying and stopping illegal money flows. Notably, in September, the European Commission proposed to give more power to the European Banking Authority, enabling better cross-border communication between authorities, a faster exchange of critical information, and stricter controls to check whether anti-money laundering laws are enforced effectively in EU member states. The EU's directive on Combating Money Laundering by Criminal Law additionally seeks to toughen penalties for money laundering and pushes relevant member states to address the risks posed by virtual currencies.

Financial regulation will likely need to be supplemented by other concerted initiatives, because:

- Banks' analysis and pooling of data for internationally-active customers will be sub-optimal where legal constraints stop it being moved across borders;
- Even the most diligent firms will be frustrated while corporate laws continue to allow structures that obscure beneficial ownership;
- Other technical obstacles impede transparency, such as incomplete information on the transaction originator in SWIFT payment messages; and
- No matter how diligent the banks are in correctly identifying and reporting suspicious activity to national financial investigation units, these units have sometimes tended to be lightly resourced and, anecdotally, overwhelmed with SARs.

A Rapid Reaction Can Avoid Making A Bad Situation Worse

Even if banks are adept at managing financial crime risks, management teams will sometimes find themselves subject to allegations that they cannot easily substantiate. This is the reality of a money transfer and transaction system where information (for example, about the originator and ultimate beneficiary) is fragmented, particularly for correspondent banks and others further down the transaction chain. Indeed, through their suspicious activity reports (SARs) banks are a key source of financial crime intelligence, but the intelligence flow can be one-way. Sometimes external parties will join the dots faster than the bank can itself.

Nevertheless, as the sharp fall in the stock prices of Swedbank and Danske indicate, the reactions of a management team and its communication become critical. For both banks, management initially downplayed the concerns, then they tried to draw a line by bringing in external auditors to substantiate or refute the allegations. However, there were missteps that, even if a bank is ultimately exonerated, have made a drama into a crisis.

Ratings Implications Will Continue To Vary

ESG risks, of which financial crime is just one, permeate many parts of our bank analysis, whether related to reputation and franchise, governance, risk exposure or solvency. Following the most recent financial crime cases, we have so far taken negative actions on Danske Bank and Swedbank. We also adjusted our view of institutional risk in our banking industry country risk assessments (BICRA) for Malta and Estonia. We did not take rating actions following other recent European bank cases, for example Deutsche Bank and ING, but continue to monitor developments. Our differentiated approach reflects that these cases vary in their fact pattern and gravity, and so financial and franchise implications for the affected banks can vary significantly. We expect that this will continue.

Nevertheless, as we've already seen in areas such as capital and liquidity management, for financial crime risk we expect that the industry standards and practices will strengthen. In this

respect, some banks will work actively and positively to support their franchise. For those that stand still, we see the investor and banking community as less willing to remain connected to banks under-delivering on governance and non-financial risk management.

Related Criteria

- Banks: Rating Methodology And Assumptions, Nov. 9, 2011
- Banking Industry Country Risk Assessment Methodology And Assumptions, Nov. 9, 2011

Related Research

- German UniCredit Bank And U.S. Authorities Settle Over Violations On Iran Sanctions, April 16, 2019
- Swedbank AB Ratings On Watch Negative Due To Implications Of Authorities' Investigations Into Alleged Money Laundering, April 1, 2019
- Bulletin: ING's Potential Shortcomings In Anti-Money-Laundering Processes In Italy Show Compliance Strengthening Is Not Over, March 19, 2019
- Bulletin: UBS Group AG Intends To Appeal French Court's €4.5 Billion Fine And Damages, Feb. 20, 2019
- How Environmental, Social, And Governance Factors Help Shape The Ratings On Governments, Insurers, And Financial Institutions, Oct. 23, 2018
- Déjà Vu All Over Again: Money-Laundering And Sanctions Woes Continue To Haunt Europe's Banks, Oct. 25, 2018
- Danske Bank Outlook Revised To Negative, Hybrids Downgraded, On Further Disclosure On Money Laundering Issues In Estonia, Sept. 25, 2018
- Estonia's Banking Sector To Benefit From Receding Imbalances But The Regulatory Track Record Is A Relative Weakness, Sept. 20, 2018
- Malta-Based Bank of Valletta Rating Lowered To 'BBB' On Increased Industry Risk; Outlook Remains Negative, Aug. 1, 2018
- How Does S&P Global Ratings Incorporate Environmental, Social, And Governance Risks Into Its Ratings Analysis, Nov. 21, 2017

This report does not constitute a rating action.

Contact List

PRIMARY CREDIT ANALYST

Giles Edwards
London
(44) 20-7176-7014
giles.edwards@spglobal.com

SECONDARY CONTACT

Bernd Ackermann
Frankfurt
(49) 69-33-999-153
bernd.ackermann@spglobal.com

SECONDARY CONTACT

Letizia Conversano
Dublin
353 1 568 0615
letizia.conversano@spglobal.com

SECONDARY CONTACT

Emmanuel F Volland
Paris
(33) 1-4420-6696
emmanuel.volland@spglobal.com

SECONDARY CONTACT

Salla von Steinaecker
Frankfurt
(49) 69-33-999-164
salla.vonsteinaecker@spglobal.com

SECONDARY CONTACT

Cihan Duran
Frankfurt
(49) 69-33-999-242
cihan.duran@spglobal.com

SECONDARY CONTACT

Francesca Sacchi
Milan
(39) 02-72111-272
francesca.sacchi@spglobal.com