ACAMS® | MONEY LAUNDERING.COM®

To Face Terror Threat, Western Union 'Evolving All the Time,' Says Compliance Chief

December 09, 2015

Terrorist attacks in Europe over the past year have done more than spur talk of new rules from the European Union. They've also prompted major financial institutions to adjust their compliance controls in an effort to root out terrorism's financial backers.

Such has been the case for Western Union Europe, according to Fabrice Borsello, the corporation's chief anti-money laundering (AML) risk officer. The money services business has worked with French officials multiple times over the year in response to shootings in Paris in January and November.

In an interview with reporter Irene Madongo, Borsello outlined the steps Western Union has taken as part of its controls to combat the financing of terrorism (CFT) and discussed recent adjustments resulting from an AML enforcement action issued earlier this year. What follows is an edited transcript of their conversation.

As a consequence of this year's string of terrorist attacks in the EU, has Western Union Europe made any changes to its counterterrorist financing program?

Our program is evolving all the time. Every time there is an attack, whether successful or aborted, we try to gather intelligence from the authorities on the vulnerabilities associated with this action, and we benchmark the identified activity versus the status of our program to see if it needs to be evolved or not. Earlier this year, I spoke at the *ACAMS AML and Financial Crime Conference* [in London] about the latest typologies regarding foreign terrorist fighters, getting into the patterns of their behavior when they transfer money or they use payment instruments. What I said in my presentation matched what appeared in the press after the November attacks. It shows our programs are working, our typologies are robust and aligned with the level of vulnerability for that type of terrorism funding that is relevant for markets exposed to this issue, like Syria, Iraq and Turkey.

Was Western Union contacted by law enforcement regarding attacks over the past year?

Western Union collaborated with the French law enforcement agencies after the January and November attacks. This collaboration is normal practice among the French banking and financial sector, and Western Union welcomes it. Actually, we were already engaged in working relationships with these agencies before the attacks took place. Indeed, contacts are maintained either on an ongoing basis or on a needs basis, depending on the governmental agency involved. Western Union values that collaboration very much and we believe it is reciprocated.

What progress are you making on your CFT programs?

We have a dedicated program that starts with usual government sanctions screening, applying the same programs as banks do. In addition, we have a terrorism risk assessment and tracking program, designed to detail the possible

behavior of foreign terrorist fighters or terrorism financiers and build targeted typologies because the potential use these people might make of our service will be following certain patterns.

The challenge of stopping terrorism funding is that, if you look at the past five years of attacks, bombing and all sorts of terrorist actions in Europe, 99 percent of the time the people who perpetrated the attack were not on the sanctions list. So it's creating a challenge for financial institutions, which then have to use criminal-risk analytics to understand such people and prevent them from using financial services like money transfer businesses to perpetrate an attack.

We look at their geographies, the amounts being transferred and their online activity, including their social networking profile, which is something important because the screening of the sanctions list is not enough. When we have their profiles and they are [deemed] suspicious, we approach law enforcement to see if they are people we should be worrying about. We are increasing the amount of financial investment in this program every year. It is part of our investment in compliance. In 2014, our overall investment in compliance was about 3.4 percent of revenues.

Have you run into data-protection or privacy issues?

When we execute these programs, we pay an equal level of attention to deterring terrorism funding and the protection of the data of our clients. As part of the money transfer industry, we cover both sides of the transactions—the information of the sender and we also have a clear view of the receiving side. For example, for transactions leaving Europe to the Middle East-Africa region, we can get advice from our AML colleagues based there, which is useful for us. We want all our work to be done in compliance with data-privacy laws on both sides.

In May of this year, the Central Bank of Ireland (CBI) fined Western Union €1.75 million for failing to adopt robust procedures when outsourcing AML and CFT compliance. The regulator also said the firm did not have adequate controls to ensure that appropriate AML training. What has Western Union done to address these issues?

The findings were related to former programs that were in place between 2010 and 2012 that have been either replaced or enhanced. Since the ruling, we have put in place programs that take into account the CBI observations. As indicated in the public notice published by the CBI, the problem was the way Western Union organized its compliance programs internationally. For example, some parts of our European compliance program were being performed with the support of other Western Union companies in Lithuania or in the U.S., all working on behalf of our Irish payment institution. CBI considered that we did not properly formalize the outsourcing arrangement between each of those Western Union entities so we have improved the program controlling the outsourcing of AML-CFT compliance functions. We have invested the necessary time, money and resources to ensure our program complies with the Irish regulation and we consider the issue closed.

Can you please give an example on the improvement?

For example, we have built a dedicated unit in Dublin that oversees the performance of each outsourced AML function working on behalf of our Irish company. This monitoring is framed around targeted performance indicators and it is supported by periodic onsite and offsite testing exercises. We have also strengthened the reporting mechanisms of this activity to the benefit of the company's board of directors.

What about training?

As you may already know, Western Union primarily distributes its financial services to the European public through a network of agents, as permitted by the Payment Services Directive. When the CBI visited some of our agent premises during that time, they expressed concern with the level of systems control on the training of the frontline associates (FLAs)—that is, the agent frontline staff servicing our clients. Although we already had a fully-effective agent training program in place, the CBI said we could have more in terms of system-control oversight of this program, ensuring that every FLA servicing clients could not only be controlled by human supervision but also by systems when it comes to the effectiveness of their training. So we enhanced our program to obtain that system-controlled assurance. As we speak, the Western Union FLAs cannot access our production system and transact if they do not have an adequate AML-CFT training on file. Our system controls their training status on an ongoing basis. Any frontline associate that is defaulting on its training obligation sees its electronic credentials cancelled and is prevented from servicing the clientele until he or she has performed the necessary trainings and passed a final electronic exam. We therefore consider this issue closed.