Wire stripping: managing compliance risk

by Jason Wingo and Julien Chanier

Recently, there has been an increasing amount of press coverage and news about financial institutions failing to comply with requirements to screen and block payments linked to sanctioned individuals, entities and countries. Many of these institutions have demonstrated an inability to monitor or prevent wire stripping.
Wire stripping is the deliberate act of changing or removing material information from wire payments or instructions, thereby making it difficult to identify and restrict payments to and from sanctioned parties or countries. Facilitating or turning a blind eye to such activity may subject financial institutions and their most senior executives to regulatory actions and criminal proceedings.

In recent wire-stripping incidents identified by US regulatory authorities, certain institutions were involved in concealing, or simply removing, true originators from transactions processed through US banks in order to avoid the sanctions-monitoring programs put in place by those institutions. A number of these institutions even went a step further, advising originating banks on how to format their transfers in a manner that would allow the transactions to avoid detection completely. As a result of their activities, the institutions were subjected to substantial regulatory fines, in addition to the reputational damage they suffered. While the actual number of true violations uncovered at these institutions was relatively small compared to their total wire activity, and also as compared to their actual transactions “stripped,” the absence of controls and compliance culture at these institutions led directly to significant regulatory actions.

With the closer scrutiny now imposed by regulatory authorities, highly public investigations and a growing number of regulatory enforcement actions, financial institutions have begun to take a more much more proactive approach to identifying, communicating and mitigating wire-stripping activities. While implementation approaches may vary, the core concepts of developing people, improving processes and leveraging available technology appear consistently when examining how best to hinder such activity from occurring within the walls of an organization, and they are necessary components of an effective compliance program.

Developing people
A recurring theme emerging from the analysis of recent events suggests that most wire-stripping activity occurs when management oversight or attitude is lax. Educating employees on the practice of wire stripping and providing them with an understanding of why it is important to identify this type of activity should be the first line of defense. However, the impact of such education will be limited if a culture of compliance does not exist within an institution, senior management is complacent or doesn’t emphasize it as a priority, or if there are concerns about retaliation against whistleblowers.

Establishing a culture of compliance at all levels within an organization is a crucial step that companies must take to empower their people to remain vigilant and cognizant of situations or activities that would be deemed non-compliant. However, a culture of compliance is not something that simply happens overnight; it requires ongoing and committed efforts from senior management. The tone from the top must thus enable compliance rather than facilitate non-compliance. Organizations can potentially prevent or mitigate wire-stripping activities by empowering highly trained employees who are adequately informed and who maintain a heightened sense of awareness toward non-compliant activity.

This said, the next questions that organizations may ask are, “What else can we do to prevent these activities?” and “How can we implement additional controls to prevent or detect these risks?”

Improving processes and controls
Defining or improving processes and controls within different functions of the organization can significantly mitigate risks and enhance the detection and prevention of wire-stripping activities over time. These processes can be implemented within customer relationship management, operations and compliance functions and typically fall into three broad categories:

- Assessments – Improving self- and independent assessment processes while simultaneously coordinating with internal audit to identify potential areas of concern in sanctions programs, including wire stripping
- Monitoring – Developing both preventive and detective processes and tools and utilizing visual analytics environments for examining large data sets to help organizations understand where future compliance risks and concerns may occur based on several different factors, such as historical issues, contextual data or industry-related events
- Governance – Improving overall governance and the level of management reporting available within an organization to measure progress against objectives and requirements

Although certain process improvements can allow organizations to increase compliance awareness, it is essential for organizations to continue leveraging available and emerging technologies for ongoing improvement of their compliance-monitoring and assessment programs. This will also permit better management of ever-changing business models and the regulatory landscape.

Leveraging technology
Organizations can implement detection processes to monitor and act upon wire-stripping activity. There are a variety of different options for organizations to consider, depending on the capabilities or limitations within their current operating environments.

Compare payment before entering or leaving the organization
In some situations, someone inside the organization may manipulate the contents of a payment transaction once it is received but prior to its being processed by the institution’s payment or settlement systems. A possible solution to identify this type of activity is to compare the payment before it enters and after it leaves the organization’s SWIFT gateway. Hash keys could be systematically generated and then compared for similarity before notifying the appropriate resources if they do not match in a particular transaction.
Mismatched hash keys may signal that wire data within the payment transaction message was changed once it entered the SWIFT gateway and before it was processed by payment systems.

Alternatively, organizations can maintain archives of all raw SWIFT payload messages either entering or leaving the organization and then create processes that would reconstruct transaction records into their corresponding SWIFT payload format. These reconstructed SWIFT messages could then be compared to the archived SWIFT messages during assessments or internal audits so that any potential violations can be identified.

Compare key attributes of payment pairs
In some cases, payments are linked to other payments, and discrepancies between these payment pairs may indicate that wire stripping has occurred. A possible detection method for this situation is to compare certain key fields of these payment pairs. For example:

- When a financial institution acts as a correspondent bank and processes payments, key attributes of incoming and outgoing messages that are expected not to be altered or changed should be compared to confirm that, in fact, the information has not been altered (e.g., beneficiary and remitter).
- When the financial institution is the remitting bank, it should be confirmed that the remitter and beneficiary fields are the same for matched pairs (e.g., MT103 and MT202-COV pairs).

Perform field level checks and detect common wire-stripping techniques
As wire stripping can also occur before an organization receives the payment, automated red-flag checks can also be a useful means of detecting potential wire-stripping activities being performed, most likely, by other institutions along the payment path. Some typical red-flag checks that can be implemented against payment transactions include:

- Checking for suspicious patterns of characters in originator or beneficiary fields, such as sequences of digits, special characters or empty spaces. (e.g., “AAAA”, “ ”, “$%#”)
- Checking for suspicious phrases usually used to conceal originator or beneficiary identity (e.g., “No name,” or “On behalf of a customer”)
- Deriving the country of the sending institution from the BIC code in the SWIFT message and comparing it to the country code of the originator’s address

Identify similar payments that have already been blocked or rejected
An additional method for detecting potential wire-stripping activity focuses on comparing previously submitted and rejected payments. This method will require financial institutions to maintain and leverage historical profiles of payment messages that were blocked or rejected. The institutions would then be able to monitor SWIFT messages against a set of payments that had previously been submitted and rejected in an effort to identify messages subsequently resubmitted without material data elements, such as originator or beneficiary name and address.

While technology, as well as any of these methods, may be leveraged for detection, it often needs to be supplemented by changes in people and processes to forestall wire-stripping activities more efficiently. Wire stripping remains a concern for regulators as it can be viewed as an overt act of non-compliance. Many institutions cannot demonstrate strong controls and validation processes to evaluate efficacy or even awareness of the potential for wire stripping; this can raise additional concerns. As several high-profile regulatory actions have occurred with regard to this issue, financial institutions would be well advised to take proactive steps to evaluate their exposure to wire stripping and begin to implement strategies to mitigate that exposure.
About the authors

Jason Wingo
Ernst & Young LLP
tel: +1 212 773 5228
e-mail: jason.wingo@ey.com

Julien Chanier
Ernst & Young LLP
tel: +1 212 773 2925
e-mail: julien.chanier@ey.com

Jason is a senior manager in EY’s Financial Services Advisory practice. He has more than 15 years of experience in the IT industry serving capital markets, retail and banking clients in the areas of anti-money laundering, economic sanctions, trading and regulatory compliance.

Julien is a manager in EY’s Financial Services Advisory practice. He has more than three years of experience in advising clients with sanction screening technology and seven years of experience in application design and development. His past professional experience also includes two years in the compliance software industry, helping top-tier US and global financial institutions implement and integrate Actimize sanction screening solutions.