FALL 2016

Treasury Update Newsletter

Treasury Security: Critical Considerations

STRATEGIC TREASURER
Consultants in Treasury

TMS|TRMS

Analyst Report

The Definitive Guide to Treasury & Risk Management Technology Solutions

- ***UNDERSTAND THE TMS-TRMS TECHNOLOGY LANDSCAPE***
- ***GAIN IN-DEPTH KNOWLEDGE OF INDIVIDUAL VENDORS***
- ***SELECT THE PROVIDERS WHO ARE THE BEST FIT FOR YOU***

Contents

Treasury Update

A Strategic Treasurer Newsletter | 525 Westpark Drive, Suite 130 | Peachtree City, GA 30269 | +1 678.466.2220

Subscriptions:
For a free subscription, visit
www.StrategicTreasurer.com/Newsletter

To unsubscribe, send your name, organization, and mailing address to
TreasuryUpdate@StrategicTreasurer.com

Advertising:
For information and rates, contact:
TUSales@StrategicTreasurer.com
+1 678.466.2220

Mission Statement:
Treasury Update, a resource for treasury professionals, is published bi-annually to raise awareness of key treasury items, issues, and events; assist with tactics and strategies; and enable treasurers and their organizations to be more resilient, effective, thoughtful, and efficient.

CHANGES IN THE CREDIT CARD INDUSTRY:

Dipping, Tapping, and NFC

The credit card industry has been evolving for many years to protect customers and merchants from fraudulent attempts. In the last one to two years we have started seeing these evolutions implemented in the United States with the introduction of the EMV or "chip" card.

The EMV acronym stands for Europe, MasterCard, and Visa, which does not mean anything to a consumer. EMV is a computerized chip inside a credit card that is an advancement of fraud protection from the magnetic strip we are accustomed to in the United States. This advancement makes it more difficult to duplicate cards and have fraudulent charges attempted on consumer accounts. This change is a new standard in the U.S. mainly due to large retail data breaches. Moving to the chip based card will reduce many of the fraudulent attempts and successes on cards.

HOW DOES A SIMPLE CHIP REDUCE FRAUD?

Let's first understand the difference between the magnetic strip card and the new EMV cards. A magnetic strip on a card holds static information that does not change. Fraudsters can duplicate that information and use it over and over, which is why they target large scale data breaches. If criminals have the static card information they can easily use that to make purchases that go undetected for a period of time. Since they are detected eventually, the large scale data they receive from these breaches is used over the course of time, maximizing their fraud success from many cardholders.

The EMV card's chip creates a unique transaction code each time it is used. If this information is breached and used by a fraudster again, the transaction will be denied because that transaction code can never be used again. This dynamic data is what makes EMV cards effective at fraud prevention and what makes the traditional magnetic strip cards primary targets.

EMV cards will continue to increase in the U.S. market as card issuers and retailers update their products and systems to comply with the card associations' change in liability. So how does this new standard in the card industry impact the market?

HOW DOES THIS IMPACT CONSUMERS?

The biggest impact this will have on consumers is increased protection because it is more difficult to counterfeit cards. This is great news for consumers. The data breaches that occur with retailers will become much less concerning because the EMV card information criminals obtain cannot be used again.

Another change is the process of payment transaction. Users are no longer swiping the magnetic strip where the card reader scans the static information on your card. The new process of inserting the EMV card into the terminal slot is called "dipping." The dipping process is very similar to swiping, with one exception. During the process of authorizing the card for the transaction, which only takes a few seconds, the card issuer creates the unique transaction code for that specific transaction. This process does take a little bit longer than the traditional swipe, but those few extra seconds are well worth the protection the EMV card provides.

Consumer habits change slowly over time, so the card associations planned for this. Let's first

understand how EMV cards are used outside of the U.S. In regions of Europe, they use what is called chip and PIN technology, which is similar to a debit card. When a credit transaction is processed, the card is "dipped," and a PIN number is entered into the terminal by the cardholder. This is two-point validation and is more secure than a signature. How many retailers do you know that check a signature on a receipt to the card or another form of identification? This is why a PIN validation is more secure. A fraudster would have to successfully duplicate a chip card and get your PIN number to make any fraudulent attempts on an EMV card.

The EMV card in the U.S. has a phased-in approach to get to the final goal of chip and PIN. Traditional credit cards use what we call "chip and signature" technology. The chip is used to create the unique transaction code, and then a signature is required to complete the purchase. This is similar to the magnetic strip process, with only one exception. Consumers are "dipping" instead of "swiping" their cards. EMV debit cards will work the same way as a traditional debit card. If you choose the "debit PIN" option at the terminal, you will enter your PIN number to verify the transaction. This is an added layer of security and validation from the consumer. If you choose credit, you will have one of two options depending on the issuing bank's system updates for EMV technology. The first is "chip and signature," which is similar to today's magnetic strip card process outlined above. The second option will be available only if the card issuer has updated their systems to handle chip and PIN technology. The process is similar to that of a debit card, in which you enter the debit PIN number instead of signing like a traditional credit card transaction. There will be variations of this process depending on the merchant, equipment, and systems.

HOW DOES EMV IMPACT BANKS OR CARD ISSUERS?

The biggest impact on banks and card issuers is financial. Card processors and issuers have to update their systems and software to accept the EMV cards and issue a new, more expensive card. Over the next 2-3 years we will see more card processors and issuers updating their systems and cards to process the more secure chip and signature/PIN transactions. The other, less measurable impact is training. Processors are at the forefront of assisting their customers (retailers) on the new processes, equipment needs, and changes in fraud liability.

It is important to note that EMV will have a long deployment before the U.S. is 100% EMV compliant. This is a slow process, and smaller banks are taking longer to roll out the changes necessary for EMV compliance due to the high financial impacts.

WHAT ARE THE IMPACTS ON BUSINESS?

EMV readiness for any business is expensive to deploy, and larger retailers with many locations find it even more cumbersome and expensive. Businesses have to train their employees and purchase new equipment that can accept the new EMV cards. This can be a complicated and costly process. Another major impact is the liability shift for fraudulent transactions. Essentially, the new liability shift means that the liability on a card-present fraudulent transaction will go to either the merchant or card issuer. The responsible party is determined by the one that is the least EMV-compliant in the fraudulent transaction. Prior to 10/1/15, the bank was the responsible party for all fraudulent charges. This recent shift in liability is a result of the large-scale breaches that have occurred from major retailers where thousands of cards were compromised.

CARD NOT PRESENT TECHNOLOGY

The evolution of payments within the last century has been nothing less than profound. In the 1940s, many smaller businesses were still accepting trade as a form of payment for for their services. Eighty years later we have advanced to where technology can allow us to tap a device or card and our payment is electronically authenticated and processed within a matter of seconds.

When we think of NFC (Near Field Communication) technology, a cell phone should come to mind. Apple Pay and Google Wallet capabilities allow us to walk around with a phone and without the need to carry a physical wallet anymore. Now debit and credit cards can be added to your phone for use where terminals with NFC can be used.

As companies update credit card terminals with EMV technology (where they can read the new chip cards), they should strongly consider terminals with NFC technology as well. This will eliminate the need to update in the future and avoid the additional costs to replace terminals again. This will immediately allow businesses to accept not only Apple Pay or Google Wallet transactions, but also cards with touchless card technology. The EMV cards issued in the U.S. today do not have the touchless card technology, but outside the U.S. this is widely used. As the U.S. adapts to the EMV cards in the next few years, we will eventually see a transition to cards with NFC capabilities.

ONLINE PAYMENT OPTIONS

When making purchases online, the options have changed dramatically as well. Like Apple Pay and Google Wallet, there is PayPal, Amazon Payments, and Dwolla.

PayPal charges the recipient customer a percentage of all payments collected online whether it is a credit card or ACH transaction from the payee. Then they pay them the net amount either via ACH or check. This can be a longer process than a simple credit card or ACH transaction direct with your customer. For the end customer this is a great option to mask their personal information and only share it with one company. This reduces the overall security risk rather than making a bunch of purchases online with your debit/credit cards.

Similar to PayPal is Amazon Payments with their retail niche. It stores your banking, credit card, and shipping information for ease of check out at numerous retail sites that are connected with the "Amazon Pay" button at checkout.

So what about other online payment options where no card is required? Dwolla Direct uses a bank network, the ACH network, or Dwolla credit for payments from individuals to other individuals, businesses, and organizations. Their fees for merchants are much less than the Paypal and Amazon Pay options because they do not use credit card processing as an option. There is no charge for a payment if it is less than $10.00 and more than $0.25. Payments are also processed faster with the use of the banking network or an ACH credit to the merchant.

What will be developed next? We may see developments coming where you will be able to add your banking information to your payment wallet and use NFC to make payments without the use of a credit card at any terminal. The way of the future is becoming touchless, and maybe credit cards will soon become a payment process of the past. ■


INVESTMENT
Region
America
Asia
Australia
Europe
2011
2012
The U.S. crackdown on Swiss banks suspected of helping
clients evade taxes by hiding income offshore has
than $1.3 billion in penalties on 80 banks in settle
involving more than 34,000 accounts that held a
billion.
In a year that saw the military government
outbreak of the deadly flu-like Mers virus
the Erawan shrine, Chinese tourists helpe
region's most-visited destination in 201
MasterCard Asia Pacific Destinations
Wednesday.
All three Thai destinations in the
ranked fifth, Pattaya eighth -
U.S. slaps $1.3B
Region
Australia
Europe
Investment

Price of Admission:

IF YOU HAVE AN ACCOUNT, YOU NEED VISIBILITY

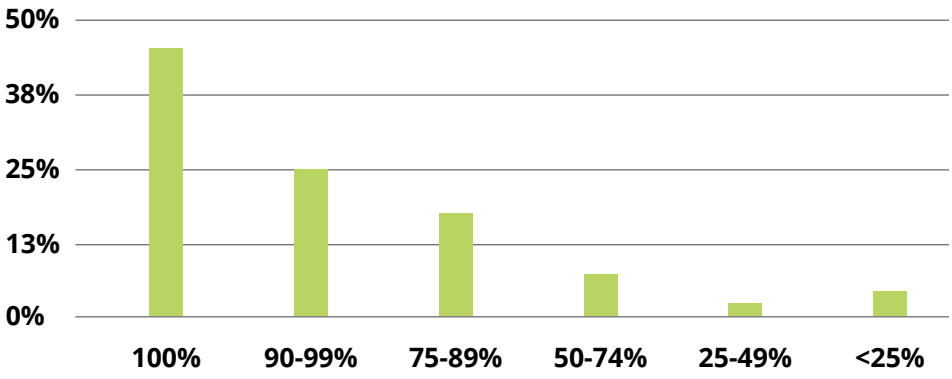
WHY IS BANK VISIBILITY IMPORTANT TO TREASURY PROFESSIONALS?

In order to make well informed financial decisions on a daily basis, your team must have accurate, up-to-date, and easily attainable bank information. Many organizations today claim to have cash visibility. However, upon further examination, their processes reveal daily visibility only to a small number of banks or bank accounts, with the majority of account information being reported on a weekly or monthly basis.

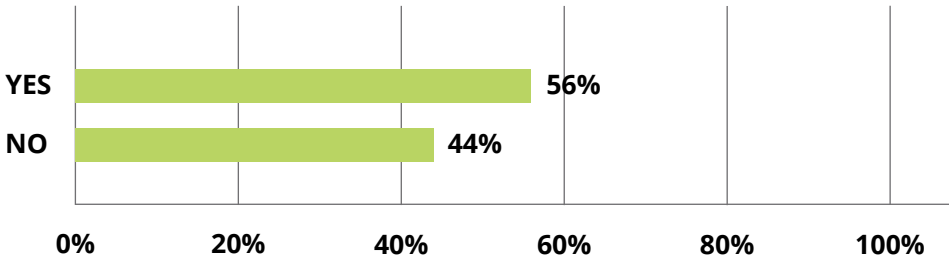
In the world of accounting, account reconciliation generally occurs on a monthly basis. This periodic approach tends to be taken for granted and can even influence the decisions of the treasury team when deciding upon an "acceptable" level of account visibility. Do we really need daily visibility? Wouldn't weekly or monthly visibility be enough? The simple answer to these questions is: In the world of treasury—if you have an account, you need to see its balance every day and, in many cases, its transactions. If you don't need this visibility, you probably don't need the account.

This approach may sound extreme to organizations who are currently operating with a myriad of accounts. However, achieving daily visibility will allow you to closely examine the transactions originating out of every account. This may lead to the realization that not all of the accounts are needed and could serve as a guiding mechanism for you in consolidating your accounts, which would in turn reduce complexity and save money on unnecessary maintenance fees. According to a recent survey conducted by Strategic Treasurer and Bottomline Technologies, less than half of the companies surveyed had daily visibility to all of their accounts. In addition, daily visibility serves as a fraud prevention mechanism; any fraudulent activity will be spotted immediately, rather than days or weeks later. In today's world, treasury operations are increasingly being chosen by criminals as a viable target for fraud. In another survey conducted by Strategic Treasurer and Bottomline Technologies, 56% of respondents indicated that their companies had experienced payment fraud attempts within the last 12 months. Having immediate visibility helps to quickly

What percentage of your bank accounts do you have visibility to on a DAILY basis (information reporting)?[1]



Has your company experienced any payment fraud attempts in the last 12 months?[2]



identify unauthorized transactions or payments and could be the difference between a massive loss or a successful prevention. In short, if an organization wants to operate effectively and have quick access to bank account information, daily visibility is a must.

EVOLVING VISIBILITY - THE TRANSITION FROM VISIBILITY THROUGH EXCEL

Thanks to modern technology, there are now more options than ever available to corporates for achieving visibility to their cash. Due to dramatic changes occurring in the Treasury Management System (TMS) landscape over the last decade, affordable TMS options have become available to midsize companies. These solutions provide excellent visibility options, which include features such as dashboards that allow a company to view its global cash position, including money in different currencies, countries, accounts, etc., and up-to-date lists of global transactions. But this enhanced functionality is not necessarily needed by every company.

Generally, most companies start with visibility through bank portals and Excel. Although these processes are heavily manual, error-prone, and time consuming, it can be difficult to determine when and how to enhance your operations. For companies operating with only a few bank accounts, it is difficult to justify the expense of a TMS. But, now that there are more cash visibility TMS offerings in play, companies with less complexity can reasonably consider the use of a TMS, as the cost point has shifted at this end of the TMS landscape. Putting small and medium businesses to the side, the number of companies using TMSs is roughly equal to the number still using Excel, as indicated by the data acquired from the Strategic Treasurer 2016 Compliance: FBAR & BAM Survey. However, we expect the number of companies using TMSs to rise as they become more affordable, business requirements continue to grow, and awareness of their capabilities spreads.

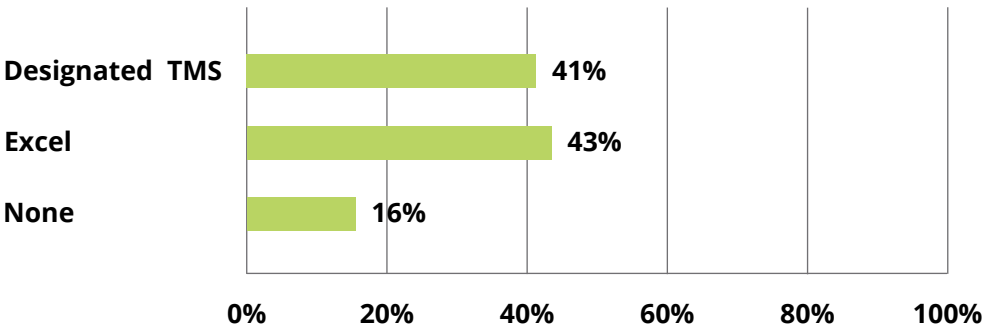
When corporates actually do jump from Excel to a TMS, we often see them present their current Excel spreadsheets to their vendor and request that they be duplicated as closely as possible within the new system. Although misguided, this approach seems to make sense at first, given that the corporate's employees are familiar with the spreadsheet format and would not be tasked with the burden of familiarizing themselves with a new layout. However, one or two years down the road, these corporations begin to realize that the new system was designed intentionally, to be functional and helpful. If your new system has been set up to mirror an old process rather than to fully utilize the built in capabilities that are available, you are severely restricting the options available to you. Understanding that it may be most efficient for your team to rethink their current processes may save you time and frustration down the road.

As you approach each potential TMS vendor, it's important to allow them to view your daily cash position worksheet and other key reports, and, in turn, see how their system will display this information for you. You need a system with analytic tools and reports, which will meet your daily needs as well as provide reports monthly, quarterly, annually, etc. that will match your organization's requirements and display information in a user friendly manner.

WHAT DO YOU NEED? WHEN DO YOU NEED AN AGGREGATOR?

If your organization does decide to implement a TMS, a key area of focus will be the aggregation of information reporting and payments. Your new system will run on information—a key piece of the puzzle which many organizations assume will be easy to get up and running. Unfortunately, this is not always the case. Instead, the implementation phase focusing on information reporting

What treasury management system do you use?[3]

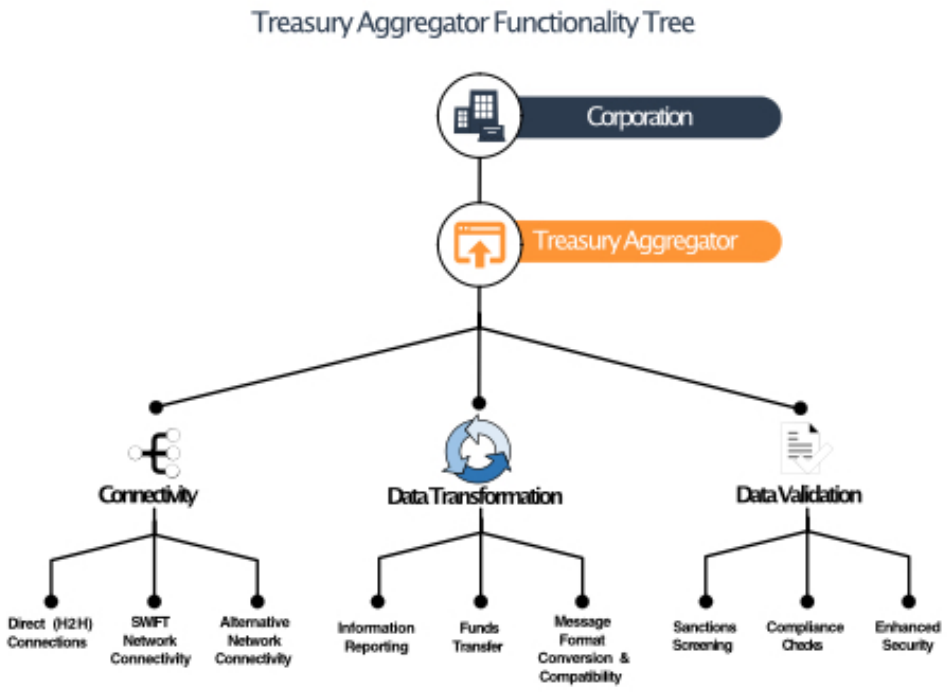


and payments can create significant delays to the overall project timeline if the magnitude and complexity of this step are underestimated. In order to be adequately prepared for this phase of your implementation, the following questions must be addressed: Will you connect directly to the TMS? Will you connect directly with SWIFT? Will you leverage an aggregator or service bureau? Your responses to these questions often require the analysis of your bank list and determining how the majority of your banks are able to connect, as well as examining your list of required payment types. Once you've narrowed this list down, you can select the most appropriate solution that fits your company's needs.

AGGREGATOR KEY ELEMENTS - WHAT TO LOOK FOR IN AN AGGREGATOR

If you've determined an aggregator is right for your organization's needs, your next step is selecting one. All selection projects are difficult—narrowing the field, sending out RFPs, interacting during demos, etc. If you know some key items to look for in the beginning, you'll be able to simplify your search.

- SWIFT Connectivity | Find out what SWIFT messaging services they can offer you, as well as whether or not you can leverage their BIC in addition to your own.
- Direct Connections | You may have banks that are not SWIFT connected, even if they appear to be at first glance. Or at some point down the road you may add a bank that isn't SWIFT connected. It's best to choose a flexible vendor that can accommodate these circumstances by connecting to the bank themselves.
- Payment Types | Ensure that you understand the payment types that will be available to you, as well as the connection methods through which each payment type will be sent. Flexibility, as mentioned above, is especially important when it comes to payments. Until recently, SEPA (Single European Payments Area) was not a requirement, but now everyone who wishes to transact in the Euro Zone must comply with it. Make sure you select a provider who can keep up with ever-changing requirements and has enough flexibility built in to accommodate any changes down the road.
- Sanctions Filtering | A solution which can perform sanctions filtering on your behalf before payments hit the bank is crucial. If a bank blocks a payment for you, it becomes a reportable event. You want to have sanctions filtering built in at all levels of your infrastructure, and your aggregator should be the last stop before the bank.
- Customer Support Model | Adding banks can be a tedious process, and you want someone who will pursue this process for you tirelessly, not leaving you to struggle with unconnected banks months after you've begun your implementation. After going live, you need to know you have a team available to help you whenever you need them, who will be responsive and aware of your specific needs.



WHY FORMATS MATTER

In today's financial messaging landscape, there are two predominant message formats in use and several less common formats, all of which allow companies to exchange messages between themselves and their banks. However, these formats don't automatically convert back and forth between each other, and thus a company must either pick one standard format for widespread use, or purchase message conversion software that can convert messages into a standard format. Both of these options involve deciding upon some standard message formats to be used by your company. How do you decide what format(s) you should pursue? You want to select a message type which will provide flexibility for your organization. Why does flexibility matter when it comes to messages? If there is a mistake in an MT message, treasury technology systems will not be able to integrate the message. SWIFT MT messages were designed in the 1970s at SWIFT's inception and today are still the most common format used by financial institutions to exchange messages. However, the MT messages have a rigid formatting structure that complicates the message delivery cycle. In light of this issue, a new and improved message format, developed according to the ISO 20022 structure, is beginning to gain traction in the financial industry as its benefits are realized.

BACK TO THE FUTURE - HOW TO HANDLE POSTDATING IN YOUR CASH POSITION

Banks in some countries do not provide consistent reporting—a real problem when you are hoping to view your global or even regional cash position on a daily basis. Sometimes, banks cannot provide the correct information in various fields which are required for your system to read the data and properly tag it. At other times, banks are functioning on old platforms that only allow them to send data when there is transaction activity. This can cause a problem for two reasons—1) many TMSs are built on balances, and if a statement is missing, the system will register this as an error; 2) you have no way of knowing if the bank simply failed to report due to an error on their part, if there is an error with your technical configuration (security keys have changed, for example), or if there was simply no activity. You can proceed with the assumption that there was no activity, but you may be deliberately overlooking a red flag that something is wrong on your side or the bank's. Another issue that is faced with some countries is postdating. The bank will record transactions based on value date rather than settlement date. They will provide you with a prior day statement at the end of each day, which appears to be accurate, but then a few days later, a revised statement will be provided. When this happens, either an alternative setup is required (i.e., weekly or monthly reporting only), or daily manual intervention (making corrections manually in the system).

CONCLUSION

Achieving visibility is crucial to operating a successful treasury department. It's important to be an advocate for visibility—to push for every account to have a purpose, and because it has a purpose, for its activity to be transparent. You may face opposition in your own department or in others, but achieving this and implementing flexible formats will be an excellent step toward future-proofing your treasury department and enabling your team to respond quickly when a crisis arises. In the modern world, you will often find the most efficient method for achieving bank visibility involves the use of a TMS and a Treasury Aggregator. TMSs and Treasury Aggregators simplify the banking processes of a corporation in many ways, including managing connections to banks on behalf of the corporate, and providing enhanced dashboards that allow a client to quickly and accurately view their cash position. For any additional information regarding how to achieve visibility for your organization, or specific questions regarding Treasury Management Systems or Treasury Aggregators, contact Strategic Treasurer. ■

[1]Strategic Treasurer & Bottomline Technologies 2015 Cash Forecasting & Visibility Survey

[2]Strategic Treasurer & Bottomline Technologies 2016 Treasury Fraud & Controls Survey

[3]Strategic Treasurer 2016 FBAR & BAM Survey

HANSE ORGA
FINANCE SOLUTIONS

SAP Partner

MAXIMUM EFFICIENCY WITH FS²

Optimize your financial processes with our innovative software family. You benefit from mobility, flexibility and comprehensive reporting while completely embedded in your current SAP® platform.

GET READY FOR THE FUTURE:

+1 (312) 620 1200 I office@hanseorga.com I WWW.HANSEORGA.COM

Practical Thinking About A Treasury Security Framework

SITUATION: CRIME DOES PAY

Security has been one of the top concerns for treasury for some years now. It is now solidly positioned as number one or number two in most organizations. This is a logical response to the situation we have reached, where crime does pay.
FIGURE 1

Since the payoff for some of this criminal activity is extremely large, criminals are investing more into their attacks on organizations. A more robust and muscular response is needed to change the calculus for the criminals back to the point where it is too costly for them to steal.

EXTERNAL AND INTERNAL SOURCES

In the 2016 Treasury Fraud & Controls Survey, it was clear that the majority of fraud was perpetrated by 3rd parties. However, the internally originated fraud, at least what was identified as internal, was still significant. Fully 35%[2] of fraud had an internal component. In addition to intentional theft, weak internal controls can contribute to an environment that allows one person to execute transactions that can damage or imperil the organization. Think of Nick Leeson for a moment. Through some rogue trading and lax internal oversight, he lost Barings Bank over $1.3B USD. This 23-year-old's actions were able to bring down a 233-year-old institution. The bank ended up being sold for 1GBP.

It should be clear that security is very important. The approach must be robust, muscular, and formal. Treasury, in all organizations, represents one of a few areas, or perhaps the only area, where lax controls, outdated security, or weak processes can gravely impact or even imperil the organization.

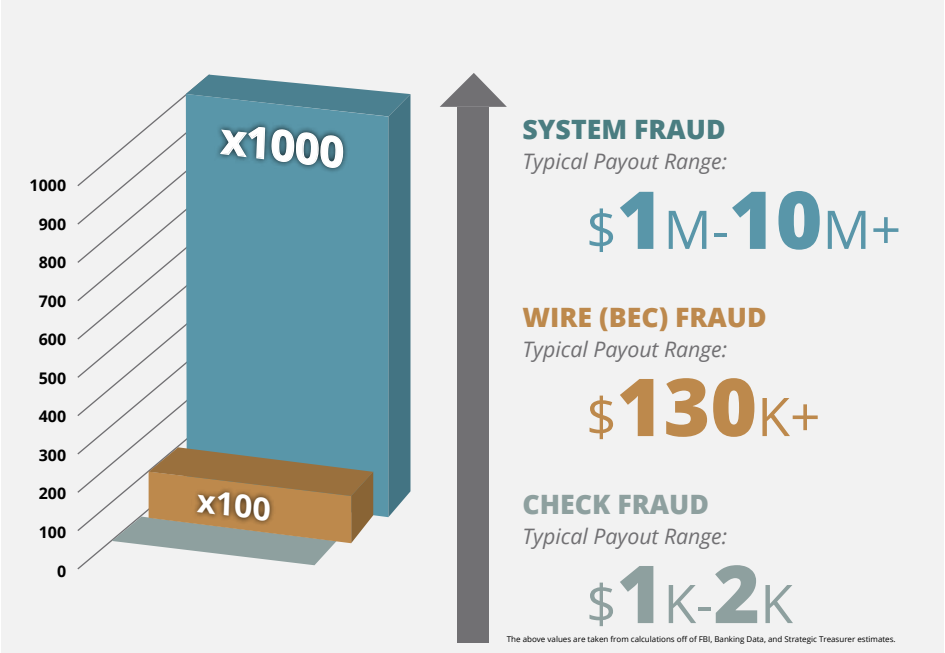
THE BUCK STOPS HERE

Perspective: treasury as the superintendent of treasury security. Taking ownership of treasury security could best be described as being the superintendent of all security that impacts treasury. This includes areas that treasury does not own. Let us examine some direct areas of responsibility and then extend the discussion to areas owned by another group such as network security or data security. Here
are some examples:

Direct Areas of Responsibility

- Controls on Banking Portals | Transfer limits and bands. Segregation of duties and dual controls. Review of audit logs for these controls. Use of repetitive setups to reduce errors. Ensuring the bank system supports the minimum controls required by the organization.
- Fraud Awareness and Monitoring | Assignments are given to monitor fraud, control, and compliance issues by specific areas and report back to the group.

FIGURE 1



The risk/reward calculus for criminals has changed as the potential payouts are larger than ever. While many corporates are on the watch for check fraud, **the larger targets remain unplanned for and vulnerable to attack.**

Indirect Areas of Responsibility

- Perimeter Security | The organization probably has an IT security or network security group with ultimate responsibility to ensure that the firewalls, routers, and network intrusion management are current, updated, and operating at optimal efficiency. That group has direct responsibility. Treasury still must know what is being done and must be comfortable that this level of security is adequate for the type of exposure the organization faces.
- Interior Security |Understanding what can be changed on an individual PC and how that can be done is one element of internal security. To connect to the network, must all machines be current on their anti-virus software and operating system patches? Can anomalous network behavior, whether arising from an external hack or from an employee attempting a criminal act, be detected and then monitored? The directory that houses payment files before being sent is locked down for access. Does an access permission and access log exist for that? Is this reviewed on a scheduled basis? Does treasury review it on a regular interval as well?

TREASURY SECURITY FRAMEWORK

A security framework details the overall security mindset and outlines the various areas that must be managed. The Five Pillars of Treasury Security cover the various steps that are taken to prepare for a security event, manage processes to reduce or eliminate fraud or the impact of security issues, and provide definition to how the system would be defended and what the response and recovery effort would look like after an event or attempt.

Two additional perspectives on security will help you put your organization on better footing: layers and ongoing enhancements. First, recognize that layers of security are vital and superior to relying on a single element. If one area is compromised, other elements can still prevent or deter the fraud or issue. Layers are harder to defeat. Second, ongoing enhancements are required because those who target companies continue to increase their sophistication and methods of attack. What was sufficient protection two years ago may be below the standards of good corporate conduct for security now. Continuing to enhance your defenses must be recognized as part of a process.

In looking at the system and near-system elements, the following graphic may help the superintendent understand the scope of his or her responsibility. This chart illustrates many of the main categories (3rd party, transport and access, perimeter, interior) and elements (incident response, access control, transaction limits, employee management). The company perspectives will be recorded in this framework document and provide the base from which policies and policy statements can be created.

TREASURY SECURITY ASSESSMENT

An annual review of your treasury security should be considered a minimal standard. At least every other year this review needs to be conducted by a 3rd party that is an expert in treasury. Having an IT group that indicates they know treasury is not adequate. Using your auditors who know accounting well but are not treasury experts will leave you with undesired gaps in your review.

The image on the next page provides some sample questions from several different areas that can give a quick sense of where you might stand in the level of security you maintain against just eight elements.

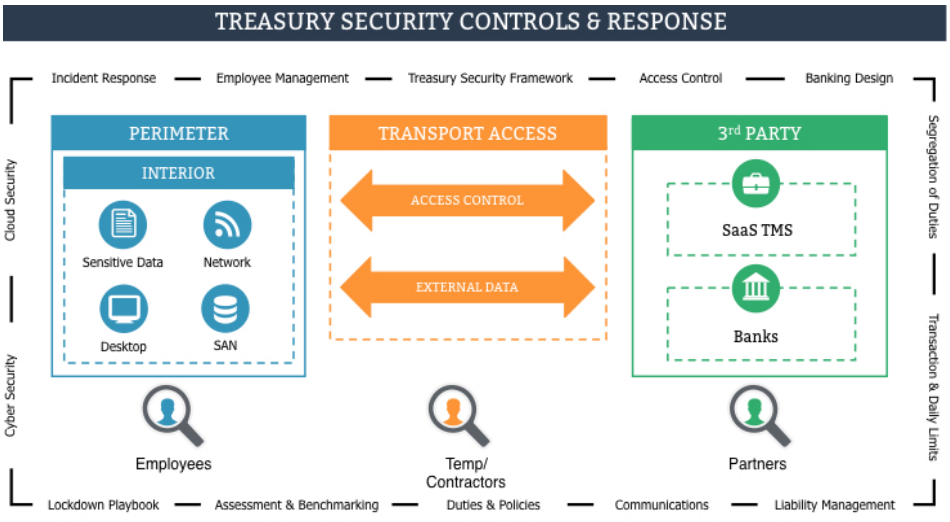
ACTION ITEMS

It is clear that the need for enhanced security is critical. Determining what should be done next will depend upon your current situation. We recognize that not everyone will begin with a full assessment of their treasury security. However, everyone can start by reviewing a few questions and providing a fair critique.

- What areas are weak, acceptable, or strong?
- What layers exist or are needed?
- How well do we know what others are doing internally in our organization or others similar to ours?
- How well do we know what others are doing externally in our organization or others similar to ours?

For those ready to embark on a more resilient defense, the following steps should ensure that your preparation, prevention, and response plans are more formal and muscular.

Crime does pay because the calculus for criminals has changed. This requires a response that changes the cost side of the equation for the criminals. If you are well on your way to developing your treasury security framework, that is excellent. If you have started, continue. If you haven't started, begin today. Stay safe. ■



This Treasury Security diagram illustrates the broad scope of treasury security operations that must be addressed through a treasury security framework. As highlighted above, a robust treasury security framework extends beyond an organization's internal systems and includes both the transportation of data and information, and the 3rd parties that information flows through or is being exchanged with.

Do you have:

- A single, current bank account management database that includes: accounts, signers, and controls?
- A formal treasury control framework or security framework?
- Internal system monitoring for fraud or unauthorized activity?
- A policy blocking the use of: BYOD, Mobile for transaction initiation?
- Systematic communication and a training program about fraud and controls for those involved in payments?

In the past year have you:

- Performed an assessment of the security for your treasury environment?
- Assigned specific fraud topic monitoring to various individuals?
- Performed initial background checks on hire for all employees, contractors/temporary workers in treasury?

Next Steps in Treasury Security:

1. Create: Treasury Security Framework
2. Perform: Fraud/Security Assessments
3. Communicate: Treasury Security Framework
4. Review: Layers by Area
5. Compare: Benchmark Key Areas
6. Calibrate: Determine Appropriate Response

[1]Strategic Treasurer & Bottomline Technologies 2016 Treasury Fraud & Controls Survey

[2]Strategic Treasurer & Bottomline Technologies 2016 Treasury Fraud & Controls Survey. 26% of respondents identified current employee involvement in fraud and 9% identified former employee involvement.

OPENLINK

Bridging the Gap

Between Treasury and Commodity Procurement

openlink.com | info@openlink.com

TMS|TRMS RELEASE WATCH 2016

The Release Watch has been a staple of the Treasury Technology Newsletter for a number of years. It shows various upgrades and enhancements released by a number of treasury technology vendors. In this issue, the Release Watch section focuses on treasury management systems and treasury risk management systems (TMS/TRMS). Future issues will include other sectors of the treasury technology landscape. Upgrades or new releases by the various vendors - either bug fixes, enhancements to features, or entirely new capabilities - are included in the Release Watch. The information provided details some of the high points of these recently issued releases or provides the reader with a sneak peek at a soon to be released functionality on a vendor and product basis.

AXLETREE

- **FILE TYPE DEFINITIONS** | Allows for the definition of the types of files to be imported as part of the forecast.
- **IMPORT TEMPLATES** | Allows for the mapping of file formats to the Treasurytree data structure.
- **FORECAST IMPORT** | Allows for the automated importation of forecasts.
- **FORECAST VIEWS** | Allows for forecasts to be viewed across daily, weekly, and monthly time horizons.
- **FORECAST ROLLOVER** | Allows for the rollover of forecasts based on historical forecasts or actuals.
- **STATEMENT VIEWER** | Provides a view of the actuals based on account statement data.
- **REPORTING** | Provides details of forecast to forecast and forecast to actual comparisons.
- **DASHBOARD** | Provides forecast analytics and graphics.
- **NOTIFICATIONS** |Provides the ability to subscribe to dynamic alerts and notifications.
- **DEBT** | Enhanced debt management module to monitor, analyze, and manage debt portfolios.
- **INVESTMENT** | Enhanced investment management module to manage investment portfolios with greater transparency and control.

REVAL

- New straight-through-processing capabilities that leverage partnerships with Oracle and SWIFT.
- Direct integration with Oracle Cloud general ledger.
- Reval Bank Connectivity Service (BCS) for large and mid-size companies.
- Bank connectivity options expanded to include EBICS, and SWIFT Alliance Lite 2, in addition to NTT DATA's gateway service and Fides multibanking services.
- Accounting and compliance capabilities expanded to encompass IFRS 9 standards, and includes new hedging capabilities.

TMS|TRMS RELEASE WATCH 2016

KYRIBA

- **HEDGE ACCOUNTING** | Developed new hedge accounting modules for FX and interest rate workflows. Full support for cash flow, fair value, and net investment hedges, prospective/retrospective effectiveness testing, and complete de-designation and reclassification support.
- **ACCOUNTING** | New capabilities for financial accounting and integrated subledger including capitalized interest and FAS52/IAS21 compliance.
- **CASH FORECASTING** | Updated variance analysis module to align budget forecasts with cash flow forecasts, advanced recurring cash flow analysis, and new view options for jointly owned accounts.
- **ADDITIONAL ENHANCEMENTS** | Supplier dashboards and funding automation, email template personalization, drag and drop file uploads, FBAR reporting, and intercompany loan withholding tax.

ORBIT

- **INDICATIVE FX RATES** | Orbit is now updated several times each day with indicative FX rates for all available currencies.
- **ENHANCED DUAL CONTROLS** | Users authorized to release payments can be restricted by specific dollar values in addition to entity and/or bank account.
- **DUAL AUTHENTICATION** | Clients now have the option to incorporate dual authentication when users access the platform.
- **INTRODUCED MID-MARKET OFFERING** | Orbit's mid-market offering is tailored to the needs and budgets on mid-market enterprises.
- **RECONCILIATION ENHANCEMENTS** | We have enhanced Orbit's reconciliation capabilities. Clients now reconcile tens of thousands of transactions daily.
- **INTERACTIVE DASH BOARD** | Orbit's new interactive dashboard provides an enhanced user experience.
- **EXPANDED SUPPORT & KNOWLEDGE BASE** | We have further enhanced our client support with additional headcount and a state-of-the-art knowledge base and ticketing system.
- **GOING MOBILE** | Our enhanced mobile capabilities provide a feature-rich experience from our clients' mobile devices.

TREASURYXPRESS

- **C2TREASURY & C2TREASURY LITE** | Maintenance releases occur weekly and upgrades are performed monthly. Upcoming 2016 releases will focus on enhancing functionality with regards to options, bonds, and swaps.
- **THE LAB** |The Lab is not a product but an online store just introduced by TreasuryXpress this year that allows clients to purchase products online for standalone use or integration with existing technology. The first product to be offered on The Lab is Forecast+, which focuses on providing a suite of cash forecasting capabilities to clients.

COMPANY OVERVIEW

This next section of the technology column provides the reader with a very brief overview of the company and a key product they offer. The description is accompanied by a screenshot of the system, workflow, cash position screen, or dashboard with the intent to provide an introduction of the firm with a glimpse of the system from at least one angle. Strategic Treasurer also provides analyst reports with more details.

REVAL

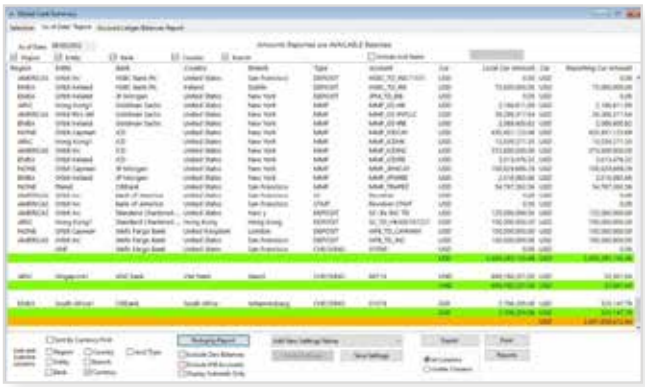
The Reval Cloud Platform was designed at inception as a multi-tenant SaaS for the corporate treasury market. With over 16 years of built-in best practices from innovative corporate treasury organizations around the world, the Reval Cloud Platform is a rich foundation of treasury and risk management (TRM) functionality. Focused on the user experience, Reval is leveraging its cloud platform to design packages in the ways various market segments consume treasury technology. Recently it launched Reval CORE™, a pre-configured, core cash and liquidity management package for mid-market companies, and Reval CHOICE™, a configurable and scalable offering selected from across the full spectrum of TRM functionality.

KYRIBA

Kyriba offers an award-winning cloud-based proactive Treasury Management System. CFOs, treasurers, and finance leaders rely on Kyriba to optimize their cash, manage their risk, and work their capital. Their secure and scalable SaaS treasury, bank connectivity, risk management, and supply chain finance solutions enable some of the world's largest and most respected organizations to drive corporate growth, obtain critical financial insights, minimize fraud, and ensure compliance.

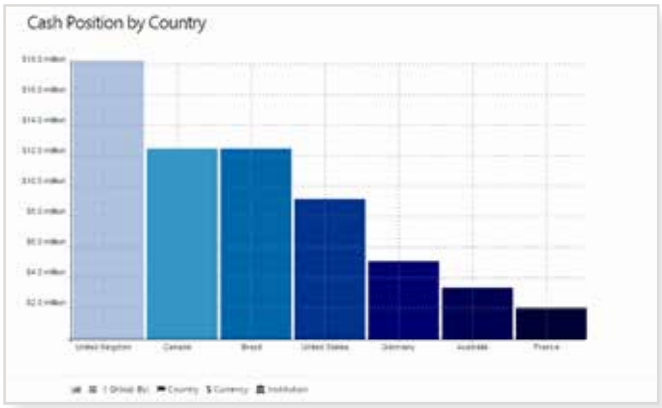
ORBIT

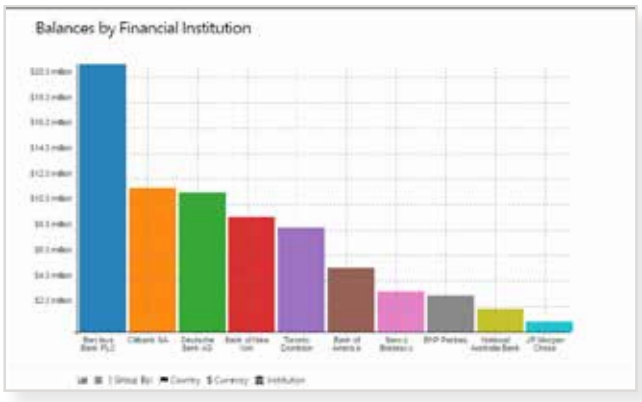
Since 1999, select Fortune 600 corporations have used Orbit to automate their treasury operations. The latest release of this robust and flexible solution is now available to the broader market. Developed and supported by corporate treasury professionals, Orbit's user-friendly interface streamlines cash and liquidity management, FX hedging, payments, bank fee analysis, bank account management, accounting, management and statutory reporting (FBAR), forecasting, and more. Detailed audit trails strengthen controls and simplify compliance. Straight-through-processing is enhanced with deep integration with ERPs, FX trading and confirmation platforms, SWIFT, and various other systems and portals.



AXLETREE

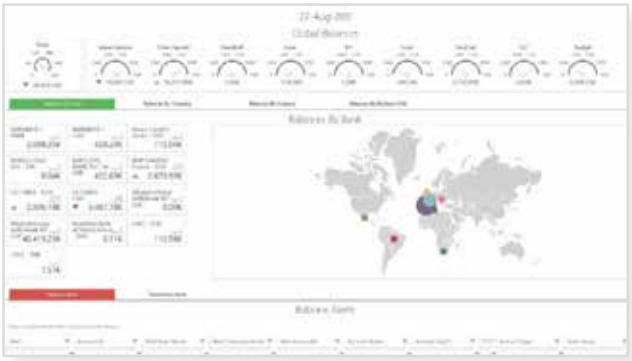
Axletree Solutions, a SWIFT Service Bureau and TMS provider headquartered in North America, has 15 years of experience in providing bank connectivity services to clients. In addition to SWIFT services, Axletree has expanded their areas of operation to include a robust Treasury Management System, Treasurytree, and message integration and transformation solution, Symmetree. Axletree was the first North American company to receive the SWIFTReady Connectivity Best Practice label (2011) and was also the first North American company to receive the SWIFT Premier Operating Practice Label (2014), both of which are notable achievements that demonstrate Axletree's position in the U.S. market.





TREASURYXPRESS

TreasuryXpress is a fully SaaS cloud-based Treasury Management System that is completely configured by the vendor. It offers exceptional functionality across cash & liquidity management, bank connectivity, payment workflow, and in-house banking. TreasuryXpress' notable features include go-live in one click, an easy to navigate interface, and report customizability across all features. TX is an ever evolving TMS with updates included in the subscription and automatically available to all users.



2016

FBAR & BAM Update

As FBAR deadlines have shifted yet another year, we have to stay aware of requirements and pending changes and track how they might impact corporates. The current deadline for individual FBARs with signature authority over but no financial interest in accounts is April 15th, 2017. These types of filers are typically signers on employer's foreign accounts, and have no personal control over being added or removed from accounts. It is common for a company to leave an individual as a signer on bank accounts even after they have left the company. It is often a burden for an already overtasked treasury team to do a full signer audit year after year, or they do complete an audit, and a breakdown occurs, and the bank does not actually remove the signers as requested.

Regardless of the circumstances, we evaluate any signers authorized with a corporation's banks at any given point during the filing year and encourage all individuals listed to file an FBAR – even if they are a former employee. In such a circumstance, it can be helpful for a 3rd party filer to handle that company's FBAR. This allows the company to continue with their daily operations and for the 3rd party to handle all documentation and tracking of current and former employees necessary for the respective filing year or years. Strategic Treasurer has conducted its annual FBAR & Bank Account Management Survey since 2014 in order to understand what corporates are doing with these regulations at the company and individual level. This year's survey involved record breaking numbers of participants, both domestic and international. As seen in the next graph, 40% of 2016's participants expect to file or have filed on behalf of their individual signers as a company.
(Figure 1)

13% of respondents have confirmed they will be outsourcing the FBAR filing to a 3rd party in order to complete the necessary electronic filing. An almost even split of participants will file internally for employees, or simply provide them the information in order to file. Depending on your number of signers on foreign accounts, it might make sense for the company to handle FBAR filing internally. A larger number such as 20+ signers might trigger the need for help from an outside company. Your corporation should take their own culture, staff availability, and number of signers on foreign accounts into consideration when deciding between filing on behalf of individuals or outsourcing the task. ■
(Figure 2)

Figure 1

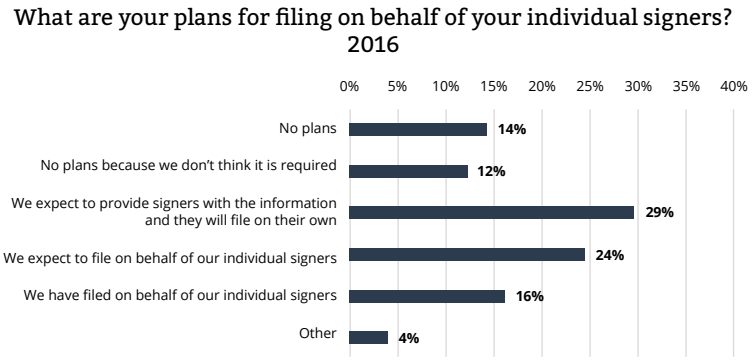
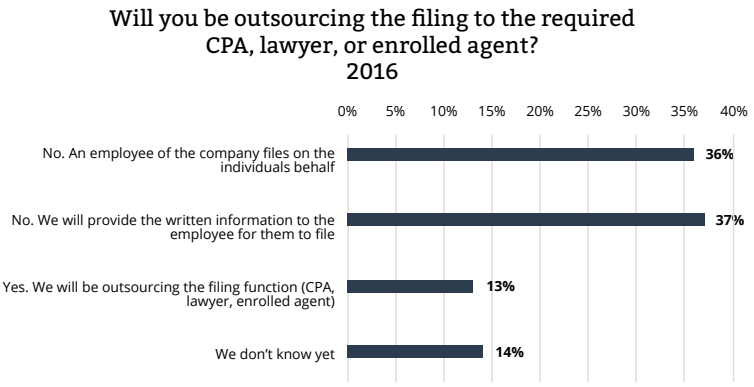


Figure 2



STRATEGIC TREASURER
525 Westpark Drive, Suite 130
Peachtree City, GA 30269
Phone: 678.466.2220

Market & Data Intelligence • 8 Annual Surveys • 75+ Annual Industry Meetings • 12 Years of Consistent Client Success • Real World Experience

Treasury Security • Compliance • Treasury & Risk Technology • Financial Risk Management • Benchmarking • Staffing • Working Capital

Email
info@strategictreasurer.com

Office
+1 678.466.2220

Web
www.strategictreasurer.com