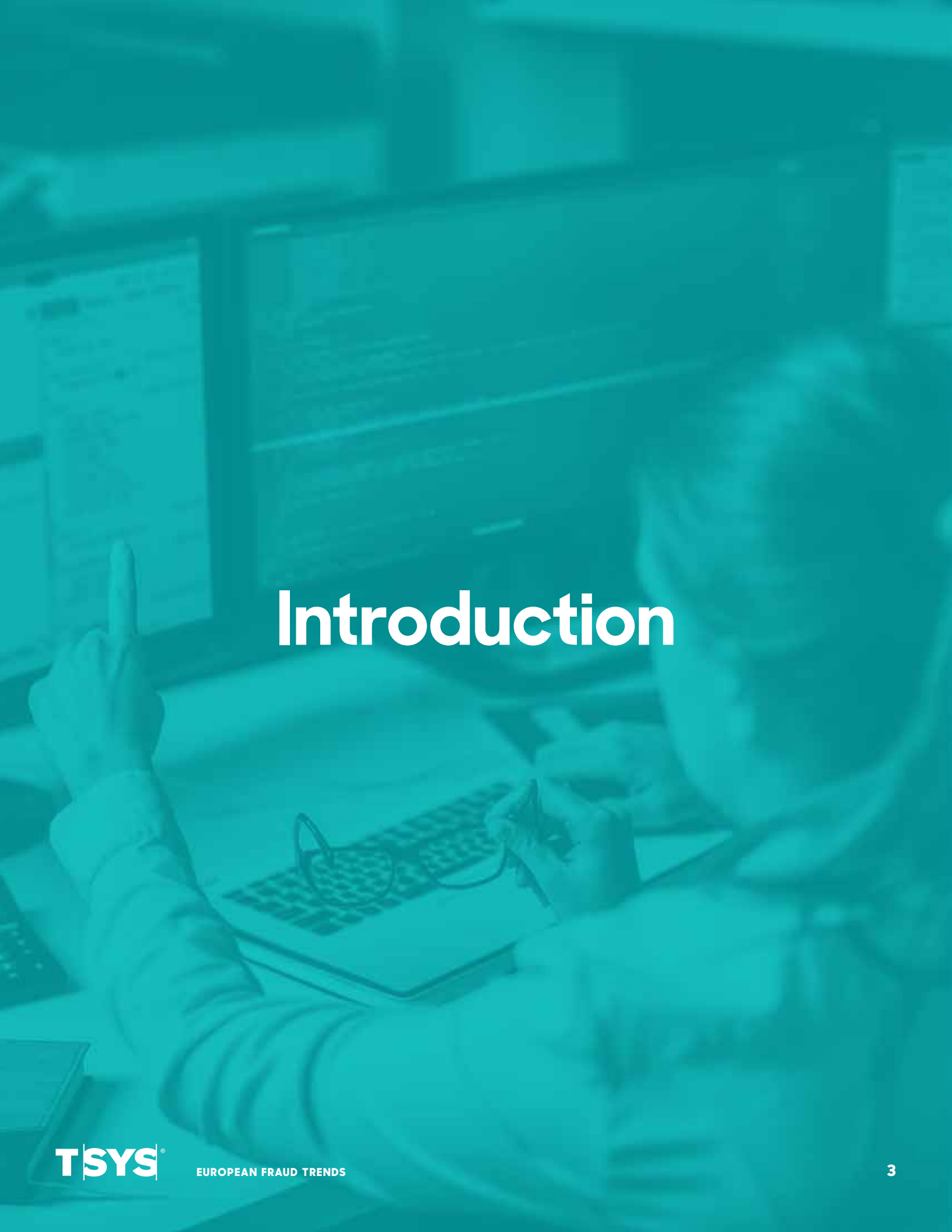
European *Fraud Trends*

A state of the union of European fraud reveals industry trends by fraud type, country and line of business

TSYS®

Table of Contents



Introduction

Fraud is a chess match and fraudsters are often one step ahead in the game.

In fact, criminals are the best they've ever been at anticipating new moves the banks and merchants might make and finding vulnerabilities in protection methods. The moment fraud management experts identify one pattern of attacks and develop a strategy to address it, fraudsters abandon the old and turn to something new.

The outcome is that fraud attacks are continually becoming more sophisticated and complex. For all the brainpower within the financial industry, it seems fraudsters can draw upon an equal amount of guile and savvy. This has created an environment in which fraud management teams need to continually invest time and resources into staying ahead of criminals, protecting their own operations and their customers' assets.

In this paper, we will

- Examine the current industry and technology trends in European fraud and what those mean for financial institutions and cardholders
- Look at some of the specific types of fraud that rapidly increased in 2016 and break those down by individual lines of business and point of sale (POS) entry mode
- Drill down by country to see where the fraudsters spent their illegally obtained money
- Share what to watch for and discuss some of the actions financial institutions should be taking now to safeguard their card business during the coming year

By Jonathan Hancock, director, fraud management solutions, TSYS global product group

Four insights from our study:

1

Card-not-present (CNP) fraud accounts for the vast majority of fraud — between 75-82 percent in the six European countries where TSYS operates.

2

Application fraud doubled as a percent of overall fraud from 2015 to 2016.

3

First-party fraud is rising quickly — and is very difficult to screen out.

4

The growing number of mobile payment applications presents unique challenges, requiring careful monitoring and evaluation.

Observations & Insights

Current Industry and Technology Trends

To begin, let's take a closer look at some of the overarching trends that are prevalent in fraud and risk management.

FRAUD MIGRATION

Fraud never stands still; it is constantly changing and evolving. The big story in 2016 was the rollout of Europay, Mastercard® and Visa® (EMV) chip cards standards in the United States. This has driven opportunistic fraudsters — who typically seek the path of least resistance — into categories with the highest potential: CNP fraud and identity theft.

ENHANCING THE CARDHOLDER EXPERIENCE

Another trend in 2016 was a shift in how cardholders view their card issuers' fraud departments. In the past, cardholders had a negative perception of fraud teams and viewed them as people who declined transactions to protect banks at the expense of customers.

On the heels of a large number of massive data breaches and other high-profile fraud attacks at major merchants, cardholders now view fraud management much more favorably. They want to know that they are being protected and are eager to be involved in the process.

PROLIFERATION OF DATA

Digital information continues to expand at exponential rates, and with it, the risk of a mass data compromise soars. Again and again, we hear about a retailer, acquirer, processor or other entity such as the internet firm, Yahoo!®, being involved in a serious data breach.

This presents a dilemma of what actions to take. If a retailer's credit cards are compromised, should the retailer implement a blanket replacement of all those cards? That can obviously be quite costly both in money and customer experience, as cardholders must receive new cards, notify merchants on auto-pay, reconfirm reservations, etc. Should tokenization be adopted as part of end-to-end encryption? EMV's standards are helping, but there are still many short-term issues during the ongoing adoption period.

ONLINE, MOBILE AND E-PAYMENTS

New ways of paying are certainly contributing to the complexity of fraud management challenges today. Mobile payments are ramping up relatively slowly, but are being adopted by more and more merchants. What are the fraud considerations for the pays?

When card issuers strive to make it simple for their cardholders to make purchases anytime, anywhere, they have to be careful that they don't also make it much easier for criminals to take advantage of these 'simplifications'.

FRAUD MANAGEMENT STRUCTURE AND CAPABILITIES

In the face of all this complexity, card issuers and processors are seeking to simplify the structure of their fraud management divisions to address issues more effectively and efficiently. In the past, fraud management teams had been very much contained in silos: one for cards, another for deposit accounts, a separate team for loans and so on.

Impact on Customer Priorities

As these trends develop, they are causing financial institutions to prioritize their actions.

With fraud threats evolving and migrating into targeted areas such as CNP and applying for new cards, financial institutions are looking to their processors and other partners to protect their organizations and cardholders from financial crimes, while allowing their businesses to continue to grow.

At the heart of it is a seemingly impossible goal: reducing the impact of fraud protections on customers by allowing them to make purchases using whatever channels and devices they choose, while limiting fraud procedures that lead to declines of legitimate transactions. This requires a level of agility never seen before.

The speed of change has also accelerated the speed of decision making required. With the velocity of payments increasing around the globe, how can institutions keep pace while introducing smarter controls into the payment process? The goal is to reduce operating expenses through increased automation and shared capabilities – while enabling cardholders to take greater advantage of self-service opportunities.

Finally, regulatory complexity is always a part of the picture. The revised EU Payment Services Directive (PSD2), which will enable consumers to use third-party providers such as Google® or Facebook® to pay their bills and manage their finances with the help of open APIs into customer accounts, as well as the latest draft of the European Banking Authority's Regulatory Technical Standards (RTS), present significant challenges for institutions. Requirements continue to be defined and interpreted, and financial institutions are looking for help in maintaining compliance while reducing their exposure to undue risks.

European Fraud by the Numbers

To gain a better understanding of fraud and its impacts to our customers, TSYS aggregated and compared fraud data from its European clients for the years 2010-2016. In 2016, gross reported fraud for all TSYS clients across Europe was €154 million, which was a dramatic increase of 25 percent from 2015. There were seven types of fraud, including lost, stolen, no receipt/intercepted, application, counterfeit, CNP and miscellaneous.

Looking at the seven types of fraud, CNP was the runaway winner, representing nearly 80 percent of all fraud losses. Counterfeit cards were the next highest category with just under 10 percent of the gross losses — although it should be noted that this has declined over the past seven years.

While €154 million is obviously a lot of money, putting those losses into context with what's happening overall with the total card-based spend casts a bit more of a positive light on the efforts of the industry's fraud management teams. If one looks at annual fraud losses as an average of the total card spend, fraud has remained relatively flat at around seven basis points since 2013 and is actually below levels recorded in 2010 and 2011.

APPLICATION FRAUD DOUBLED IN 2016

While CNP and counterfeit fraud led the way in 2016, one development that should catch the attention of fraud managers is that application fraud as a percent of overall fraud doubled from 2015 to 2016.

When someone fraudulently applies for and is issued a card, it is very challenging to contain the losses. Transactions are not recoverable, and they are difficult to profile and screen out once a fraudster has a card in his or her hands. So, while application fraud still represents a very small percentage of the total losses, this is an area where additional diligence on the policies and procedures around screening applicants, verifying identities and conducting risk assessments could pay dividends in reducing fraud losses.

BREAKING DOWN FRAUD BY COUNTRY

TSYS does business in six European countries: Germany, Ireland, Italy, the Netherlands, Switzerland and the UK. Fraud risk varied from one country to another, but CNP fraud leads by huge numbers everywhere. It ranged from a low of 75 percent to a high of 82 percent, with an average in all six countries of 79 percent.

Other interesting observations included:

- The UK had much less counterfeit card fraud — only six percent, half that of the next countries observed — Italy and Switzerland.
- Unfortunately, the UK had a considerably higher percentage of application fraud than the other countries — representing six percent of the total fraud — while in the other countries application fraud was either one percent or less.
- Fraud using stolen cards was higher in Italy (eight percent) and Switzerland (six percent) than in the rest of Europe.

We also investigated which countries were on the receiving end of the fraud that originated in the six European countries we analyzed.

- Not surprisingly, the United States was the leading recipient of fraudulent transactions from Ireland, Germany and the Netherlands with between 15-22 percent of the transactions going there. For Switzerland and the UK, it was the second biggest recipient and the third for Italy. This is likely because some of the largest online retailers are based in the United States.
- For Switzerland, just less than 20 percent of the fraudulent transactions were being received in the UK.
- In Italy and the UK, the number one location of fraudulent transactions was in its own back yard — with nearly 20 percent of the UK's bad transactions taking place domestically, and approximately 27 percent of Italy's fraudulent transactions occurring at home.

DIVING DEEPER INTO THE DATA

We took the seven key types of fraud and categorized them within consumer, commercial or debit lines of business, depending on where they were most prevalent.

As one might imagine, application fraud is almost exclusively the domain of consumer cards because applying for a commercial card is a much more rigorous process than applying for a consumer card. Debit cards make up a higher percentage (11 percent) of stolen card fraud than in any of the other categories. Debit cards are also vulnerable to CNP and counterfeit transactions, but account for virtually none of the other types of fraud: application, lost, intercepted and miscellaneous.

We further broke the data down by merchant types to come up with the top-10 targets of fraudulent purchases. The merchant categories, in order, included:

- Travel agencies and tour operators
- Electronic sales
- Lodging — hotels, motels and resorts
- Financial institutions — ATMs and cash
- Grocery
- Department stores
- Betting and gaming
- Men's and women's clothing
- Insurance sales, underwriting and premiums
- Miscellaneous and specialty retail

Perhaps unsurprisingly, this means fraudsters are typically buying high-value electronic goods, luxury travel, nights at hotels and motels, cash and food — followed by the other categories.

We also examined how the fraud was perpetrated by POS entry mode. It was quite clear is that e-commerce primary account number (PAN) entry led the way with more than 50 percent of the fraudulent transactions, followed by manual/key entry — most likely as part of mail order or telephone order transactions.

Worldwide Adoption of EMV

Europe led the way in the adoption of the EMV global payment standards for chip cards, and this continues to be reflected in the widespread use of EMV across the continent.

In Europe, 86 percent of the cards and 99 percent of the transactions comply with EMV. Contrast this with Asia Pacific and Oceania where only 38 percent of the cards and 60 percent of the transactions are in compliance – or the United States where 51 percent of the cards are now chip cards, but a scant 20 percent of the transactions comply with EMV standards.

Still, as bad as the U.S. percentages look, just two years ago, only seven percent of its cards were EMV-approved chip cards and less than one percent of the transactions complied with the standards.

The move to EMV is acting as the driving force behind the rapid rise in CNP transactions. With old mag-stripe cards, if a fraudster in the UK wanted to use counterfeit cards to purchase goods and services, he was likely to look to the U.S. market. As more of the United States converts to the EMV standard, this will redirect more and more of the fraud online into e-commerce transactions where no swipe is involved.

What to Watch for

Fraud Outlook

So where does this leave card issuers and their fraud management teams? As we mentioned earlier, CNP and application fraud lead the way for focus, but other concerns require additional scrutiny as well:

- ***CNP is the biggest challenge.*** 3D Secure authenticated payment, developed by CA Technologies® and implemented in various forms by Visa, Mastercard and American Express®, promises to improve the security of online transactions. But merchant adoption globally remains very low, and this hurts both the cardholder and card issuing institutions in terms of growing fraud losses.
- ***Application fraud is an increasing problem.*** It doubled based on a percentage of overall fraud from 2015 to 2016, and because fraudsters actually hold a card issued by a financial institution, it can be very difficult to control.
- ***First-party fraud*** – where a cardholder claims that he or she simply didn't make a given purchase – is also rising and is quite a challenging issue.
- ***In the area of mobile payments,*** the proliferation of mobile apps needs to be carefully monitored and evaluated from a security standpoint.
- ***PSD2 is coming in January of 2018,*** and this will have significant implications for card issuers and cardholders. Under PSD2, access to accounts will become almost ubiquitous. For issuers, PSD2 is going to introduce a whole new layer of competition and complexity into the payment process – making it easier to access consumer accounts for payment competitors such as Google or Facebook, while unfortunately offering criminals another entry point for fraud.
- ***Last, while completion of the EMV migration process may still be a way off in the United States*** – primarily in terms of widespread merchant adoption – the U.S. banking industry is making steady progress. Visa's ATM standards and the Visa/Mastercard automated fuel delivery (AFD) POS liability shift are scheduled to come into force in October of 2017. This will be another major engine driving the universal adoption of EMV standards in the U.S.

Where to Turn for Fraud Leadership

As a leader in bank issuing and acquiring as well as merchant and prepaid solutions, TSYS unlocks opportunities for payment providers, businesses and consumers.

We offer a comprehensive portfolio of products and services to safeguard payments and help issuers combat fraud. Just one of the ways we do this is through TSYS Foresight Score℠ with Featurespace®. It incorporates machine-learning capabilities to deliver significant advantages in the fight against fraud. When used in conjunction with existing scoring models, as part of a comprehensive fraud strategy you'll be better equipped to accurately spot and prevent more types of fraud including new and previously unknown fraud types, especially CNP fraud.

It relies on Featurespace's powerful adaptive behavioral analytics engine – ARIC® – which combines Bayesian statistical algorithms with the latest in machine learning to accurately identify fraud at the individual customer level. Other benefits include:

Real-time data collection
Predicts customer behavior and score individual transactions in real time

Reduced operational costs
Reduces manual intervention for lower costs in time, money and resources

Fewer false positives
Detects anomalies at the customer level, spotting fraud without disrupting the customer experience.

Self-learning technology
Learns more with every new data set for enhanced precision in detecting and preventing fraud

Unmatched security
Protects data, which never leaves TSYS' secure, controlled environment

ABOUT TSYS

TSYS® (NYSE: TSS) is a leading global payments provider, offering seamless, secure and innovative solutions across the payments spectrum – from issuer processing and merchant acquiring to prepaid program management . We succeed because we put people, and their needs, at the heart of every decision. It's an approach we call 'People-Centered Payments™'.

Our headquarters are located in Columbus, Ga., U.S.A., with approximately 11,500 team members and local offices spread across 13 countries. TSYS generated revenue of $4.2 billion in 2016, while processing more than 25.5 billion transactions. We are a member of The Civic 50 and were named one of the 2017 World's Most Ethical Companies by Ethisphere magazine. TSYS is a member of the S&P 500 and routinely posts all important information on its website. **For more, visit us at tsys.com.**

CALL US:

Africa
+27.21.55.66392

Asia-Pacific
+603 2173 6800

Commonwealth of Independent States
+7 495 287 3800

Europe
+44 (0) 1904 562000

India & Southeast Asia
+911204191000

Latin America & the Caribbean
+55 19 3112 2700

Middle East
+971 (4) 550 3100

North America
+1.706.649.2310

To learn more:

contact 1.706.649.2307
or email sales@tsys.com.


twitter.com/tsys_tss


facebook.com/tsys1


linkedin.com/company/tsys

TSYS®