CyberSource®
the power of payment

CYBERSOURCE Online Fraud Benchmark Report

2016
Southeast Asia Edition

Published September 2016

INTRODUCTION

Fraud management is an essential component of running an eCommerce business because it is intrinsically connected to a merchant's bottom line. To understand what merchants in Southeast Asia (SEA) are concerned with in fraud management, CyberSource commissioned an inaugural online payment fraud survey for this region.

A total of 152 merchants took part, representing an even spread across the top five SEA eCommerce markets in size and growth rate—Indonesia, Malaysia, the Philippines, Singapore, and Thailand. In terms of eCommerce revenue, 51.3% have an annual turnover of less than US$5M, while 48.7% have an annual turnover of US$5M or more.

Participants were interviewed in person and via telephone by East & Partners Asia over a four-week period in December 2015. This report summarises their responses in three sections:

- SEA online fraud benchmarks with country analysis
- Strategic challenges and priorities for fraud management
- Overview of mobile commerce and mobile fraud risks

About East & Partners Asia

East & Partners Asia is a leading banking research and advisory firm providing the financial services industry with independent, market wide research, analysis and customer insight on the institutional corporate and business banking markets.

SECTION 1

Regional Online Fraud Metrics And Country Analysis

SEA ECOMMERCE A BURGEONING MARKET

Respondents in SEA have an annual online revenue of US$4.95M on average, accounting for 29.1% of total revenue. The five countries have varying amounts of online revenue, yet the range of eCommerce contribution to gross revenues was less wide. Singapore, the survey's top online earner at US$12.1M, saw eCommerce make up 36.5% of its total revenue. Indonesia, the smallest earner with US$1.44M, had 22.1% of its total revenue come from eCommerce.

The merchants surveyed have an average of 5.2 years of eCommerce experience. Interestingly, the amount of eCommerce experience was found to be proportionally related to a merchant's online earnings: Merchants in Singapore, the survey's highest online earners, are also the most experienced with 7.4 years under their belt, whereas merchants in Indonesia, the smallest online earner, have the least experience among respondents at 3.6 years.

The findings prove that eCommerce is prevalent and well on its way up throughout the five countries in the region. Companies hence cannot afford to wait and see before hopping on the digital bandwagon to boost sales, which must include fraud management as the overall market, along with consumers and fraud risks, continue to evolve.

32.9%

Expect No Change in Future Revenue Loss to Fraud

1 IN 4 EXPECT GREATER FRAUD LOSSES

Nearly a third (32.9%) of SEA merchants do not expect their revenue fraud loss to change compared to the year before. As for the rest, about 27% anticipate a greater loss, 22.4% do not know, and 17.8% think it will be lower.

In Singapore, most merchants (53.3%) expect no change in revenue fraud loss, though a substantial number (33.3%) predict a lower loss. Few think it will be a greater loss (6.7%) or do not know (6.7%). Indonesia had the opposite results: Those who do not know (36.7%) or expect greater loss (30%) were the majority, rather than those expecting no change (20%) or lower loss (13.3%).

Similar to Indonesia, Malaysia, Thailand and the Philippines all saw the bulk of their merchants expect either greater revenue fraud losses or no change, and fewer of them who either do not know or expect smaller losses.

Considering one in five merchants in SEA are uncertain about future fraud losses, and one in four anticipate greater losses, the importance of having fraud visibility in eCommerce operations cannot be underestimated. Visibility is key to helping merchants build and enhance a fraud management strategy that supports their business goals, instead of unknowingly severing them.

Respondents in SEA reported an average of 2.8% of online revenue loss due to fraud, within which disparities among the five countries were seen. Indonesia (3.4%) had the survey's highest online revenue fraud loss rate, with the Philippines (3.3%) a close second. They were followed by Malaysia (3.0%), Thailand (2.8%), and Singapore (1.5%).

The survey also found that smaller companies, those below US$5M in annual turnover, reported nearly double the revenue fraud loss rate (3.6%) of larger companies (1.9%), those earning US$5M or more. This could be due to a learning curve in developing capabilities in fraud management as well as an increasing need to stem fraud, since the impact of fraud moves up in tandem with a bigger volume of sales.

One reason behind a high revenue fraud loss rate could be the lack of automated screening. This is essential to accurately filter good inbound orders from fraudulent ones, so merchants can stop bad transactions early on. During times of peak periods such as online holiday shopping, the volume of incoming orders and fraud risks multiply, making rapid and reliable fraud detection paramount.

Furthermore, revenue fraud loss has a close association with profit impact. A low revenue fraud loss rate means merchants get to retain more of the bump in sales revenue for more profits, and all the better if their overall fraud management is efficient to keep costs low.

2.8%

Online Revenue
Fraud Loss Rate

IS IT TOO HIGH
OR TOO LOW?

REJECT BASED ON DATA EVIDENCE, NOT SOLELY ON FRAUD SUSPICION

Merchants in SEA said they reject about 2.5% of orders annually based purely on fraud suspicion. Singapore (4.7%) had the survey's highest order rejection rate. Malaysia (2.5%) was second, Thailand (2%) third, and then Indonesia (1.7%), and the Philippines (1.6%).

Incidentally, the survey uncovered that the more experienced the respondent—like those from Singapore—the greater the tendency to reject orders. A possible explanation might be a lower risk tolerance as the size of the business increases, given how the potential impact of fraud rises alongside greater sales volume.

That said, an order rejection rate is less a reflection of true fraud risk than it is a knee-jerk reaction to fraud. Merchants must take proactive steps to avoid costly individual bias, so that they do not mistakenly reject a vague but genuine order, or allow a stealth fraudulent one to go through their gateway undetected.

That is why it is crucial for merchants to have oversight on the methods and criteria used to reject orders. One way is to always access valuable data to have both visibility and accuracy to correctly spot bad orders. This step is vital for businesses to remain one step ahead of fraudsters even if the latter finds new ways to exploit gaps in payment systems.

2.5%

Order Rejection Rate

8.6%

False Positive Rate

1 IN 10 REJECTED ORDERS ESTIMATED TO BE WRONGLY DISMISSED

For the SEA merchants surveyed, the percentage of rejected orders that respondents believe to actually be valid—also known as false positives—was found to be 8.6%. This rate is cause for concern for two reasons. First, one in every 10 orders was erroneously turned down, leading to lost revenue, which is all the more salient if the transaction figure was significant. Second, a genuine shopper had a negative experience of getting his or her order dismissed, a kind of “customer insult” that can cause a drop in return visits or satisfaction ratings.

Tackling false positives is a quick way for merchants to focus efforts to become more strategic and avoid costly oversight by reducing the odds of wrongly rejecting valid orders in the first place. One way is to automate fraud detection and sorting with effective screening rules, which will block fraudulent orders and simultaneously speed up acceptance of good orders passing through.

The false positive statistic is culled from known complaints or feedback from customers, if the customers are willing to give feedback in the first place. Hence it is important to implement a feedback loop, so that any customer complaint can be traced back to the initial reject case and be classified as a false positive. Otherwise merchants will have no visibility whatsoever to track false positives to reduce them, a situation that 4.6% of survey respondents are currently facing.

HIGH POST-REVIEW ACCEPTANCE BELIES INEFFICIENCIES

15.9%

Manual Review Rate

Respondents in SEA manually screen 15.9% of all their orders for fraud yearly, with those in Indonesia doing the most manual reviews (19.7%), and Singapore the least (10.5%).

With a 15.9% average review rate, it would seem at first that SEA merchants are not overdoing manual reviews. However, the time and effort spent by review teams are arguably used inefficiently, because 88.7% of manually-reviewed orders end up being accepted. This is most apparent in Singapore, where merchants do the fewest manual reviews, but accept 92.4% of those orders.

Singapore is not alone. Malaysia (91%) had a similarly high post-review order acceptance rate, and the rest of the countries were not far behind. Indonesia accepted 89.3% of its manually reviewed orders, followed by Thailand (87.1%), and the Philippines (85.6%).

What these results suggest is having the right tools at hand only goes so far. Merchants need to know how to make most out of them for greater effectiveness, not just output. For instance, writing smarter fraud rules is pivotal in improving the precision of automatic screening. This way, fewer and only the most dubious orders are routed to manual review teams. It also helps increase the speed of customer service, so as to not test the patience of valid shoppers.

3-D SECURE IS NOT AN END-ALL FRAUD PROTECTION STRATEGY

One-time payer authentication not a substitute for fraud management

Survey respondents generally treat 3-D Secure as complete protection against fraud. Based on a scale from 1 to 5, with 1 being the most confident and 5 the least, they gave a rating of 2.20. Merchants in the Philippines (1.99) have the most confidence in 3-D Secure, followed by Indonesia (2.04) and Thailand (2.07). Those in Malaysia (2.33) and Singapore (2.56) were a bit less confident.

Depending on 3-D Secure alone prevents businesses from seeing the full picture of fraud and its financial implications. 3-D Secure is first and foremost a payer authentication mechanism with two important functions: It verifies a cardholder's identity at the time of a transaction, and shifts the liability from the merchant to the cardholder's bank. But it is not an end-all substitute for fraud prevention and management.

Rather, 3-D Secure works hand in hand with fraud management, the latter being a broad strategy about overall detection of fraudulent behaviour and transactions. After all, the business impact of fraud has several manifestations besides credit card misuse, such as direct revenue losses caused by false positives or high operating costs due to review staffing. Merchants must therefore look at fraud management as an end-to-end process of interconnected parts.

67.1%

Plan to Increase Fraud Budgets

LACK OF VISIBILITY CAN HURT BUDGET MANAGEMENT

Close to all respondents (92.1%) in the survey have no inkling as to how much online revenue—excluding actual fraud losses—ends up being spent to mitigate fraud. This paints a sobering picture that very few businesses have visibility over the total costs they rake up in fighting fraud. Not knowing where and how much money is consumed by management of fraud implicates budget planning, and becomes especially problematic if respondents decide to increase fraud budgets.

The survey did indeed find that more than two thirds (67.1%) of merchants plan to beef up their fraud management budgets over the next 12 months. Around 30.9% will maintain their current budgets, and just 2% are planning a decrease.

Increasing the fraud budget is not necessarily a step back to making overall fraud management effective. What is crucial is merchants have enough visibility on their fraud-related expenditure, otherwise optimising their budget and investments becomes more complicated than it needs to. Ultimately, greater discernment and control on fraud expenses make it easier to prevent profits from sliding off the bottom line.

SECTION 2

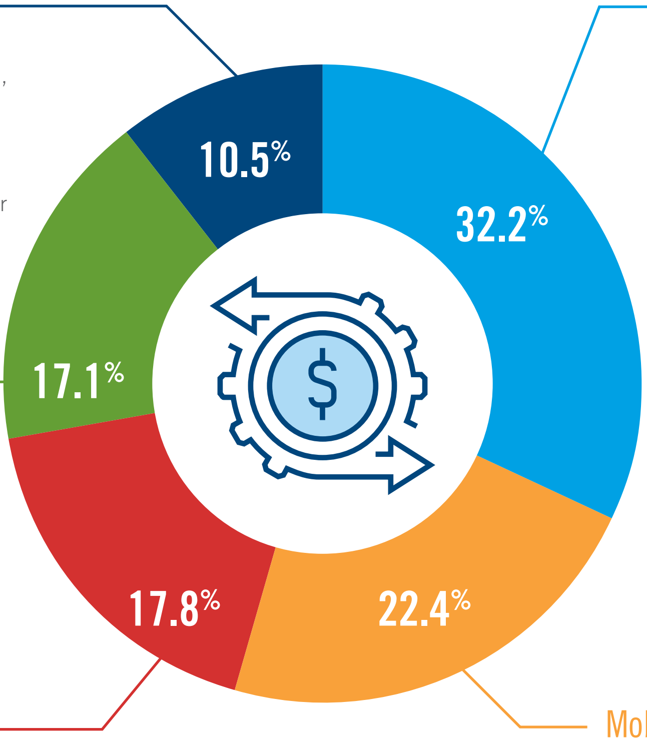
Top Challenges and Priorities in Online Fraud Management

THE BIGGEST FRAUD CHALLENGES OF SEA MERCHANTS

To find out which areas of fraud management merchants in SEA are most concerned about, the survey gave participants a set of five different fraud challenges and asked them to pick the one that was their biggest challenge in the last 12 months.

This turned out to be fraud management tools, chosen by a third of all respondents. Improving tools is a quick way to help overall fraud mitigation, so placing the most emphasis on the operations side of things makes sense for merchants. They then might proceed to more specific issues (mobile fraud and foreign cards) or broad underlying ones (expertise and costs), which would explain why fewer respondents selected those as their number one challenge.

What was your biggest fraud management challenge in the last 12 months?



Cost

Respondents do not seem too fazed with having to spend more to fight fraud, as seen by the earlier result of bigger fraud budgets planned. While costs are unavoidable, a good fraud strategy is one that not only minimises fraud costs, but also maximises order acceptance for bigger margins.

Fraud Management Tools

The top-voted challenge by all respondents was also the biggest issue for those in the Philippines (45.2%), Singapore (43.3%), and Indonesia (30%). Using better, more appropriate tools helps merchants quickly reap efficiencies and savings, which explains for the bulk of merchants' votes.

Fraud Management Expertise

Keeping up with fraud know-how requires time and energy that merchants running and growing an online business do not have on hand all the time. Yet, fraud management expertise is invaluable to help achieve business goals, be it keeping profit margins and accelerating market expansion.

Foreign-Issued Cards

Though this ranked third overall, it was the top challenge for nearly one third of respondents in Thailand (30%). Chargeback resolution of foreign cards can be more complicated, so merchants may resort to doing more manual reviews or order rejections, which can affect their revenue.

Mobile-Related Fraud

Mobile fraud was the biggest challenge for a quarter of all respondents as well as a third of merchants in Malaysia (35.5%). This may be linked to unfamiliarity on how to spot fraudulent behaviour or write screening rules specifically around mobile-based transactions.

TOP PRIORITIES FOR FRAUD MANAGEMENT IN SEA

The survey also looked at what upcoming priorities SEA merchants have for fraud management. Shown a list of five strategic goals, participants had to rate each goal as a high, medium or low priority of theirs over the next 12 months.

Goals that got the most number of high priority nods were about improving operational efficiencies in manual review and fraud detection. Next were broader aims of omni-channel monitoring as well as data analysis. Last place was end-to-end strategy and optimisation, picked by the least respondents as a high priority. Like the earlier results regarding respondents' fraud challenges, their choice of priorities here prove merchants are generally most inclined to deal with operations as a first step.

This table shows the five strategic goals ranked in descending order of high priority votes, as given by respondents.

High priority goals for fraud management OVER THE NEXT 12 MONTHS

59.9%
Streamline manual review tasks and workflow

Three in every five survey respondents selected this as a high priority. Coupled with the earlier finding that 88.7% of orders get accepted post-review, merchants in SEA are clearly making a beeline to be more efficient in manual reviews, since it is resource-intensive.

54.6%
Improve automated detection and sorting accuracy

Identifying and weeding out invalid transactions at the earliest instance enhances processes downstream, such as lowering the reliance on manual reviews. It also means merchants can increase their order acceptance rate, without the risk of raising their fraud rate.

53.3%
Track eCommerce fraud and fraud metrics across all channels including mobile

Monitoring fraud across all channels lets a merchant objectively evaluate vulnerabilities and how they perform on each one. That way, they stay informed of which gaps need fixing, and can do so in timely fashion, without unintended disruptions to running their business.

45.4%
Capture and analyse the right data and use it effectively

With relevant data insights, merchants can refine their fraud management practices for greater effectiveness, benefitting the overall business. For example, analysing historical or industry-wide transaction data helps them improve existing fraud rules to enhance detection.

22.4%
Optimise fraud strategies and detection tools for every channel we operate

Meeting this goal demands time and effort. The payoff is a well- integrated and reliable fraud management system that is rigorous enough to detect various traces of fraud, and also nimble in accepting more good orders quickly for sustainable growth and profits.

SECTION 3

Overview of Mobile Commerce and Mobile Fraud Risks

MOBILE COMMERCE NASCENT IN SEA BUT FRAUD RISKS EXIST

Mobile channel adoption by merchants is at present sporadic in SEA, according to this survey's findings. Since mCommerce is in its infancy—some countries are albeit slightly ahead of others along the adoption curve —understanding of mobile fraud risks and the techniques and tools to combat them is generally also at the nascent level.

That looks set to change as more consumers in the region pay for online purchases via their mobile devices, largely driven by growth in mobile broadband subscriptions and smartphone ownership that is expected to hit 230 million units by 2017[1], according to Forrester Research. Consequently, cross-channel fraud management of online and mobile platforms will only rise in importance for eCommerce players—the survey found nearly two thirds of respondents know what their mobile fraud rate by revenue is.

[1] Forrester, "The Mobile Payment Opportunity in Southeast Asia: The Race for Mobile Payments Is Heating Up", October 2015.

41.1%

Have No mCommerce Adoption

FOR THOSE WHO DO, MAJORITY OWN AN APP

Almost half the respondents have no mCommerce presence (41.4%), defined by the survey as a mobile site or an app. For the rest who have adopted the mobile channel, the most common method was an app (26.3%), rather than a site (19.1%). Far fewer merchants own both (13.2%).

Mobile apps did turn out to be the most popular medium for merchants in all five countries, even when each country showed varying degrees of overall mCommerce adoption. Singapore took the top spot with 90% of its merchants already on board the mobile platform: app (40%), site (33.3%), both (16.7%), neither (10%). Malaysia was second: app (29%), site (25.8%), neither (25.8%), both (19.4%).

Interestingly, in Thailand, its number of merchants who have apps (30%) exceeded Malaysia's figure. Less common were a mobile site (20%) or both (10%), while the reminder (40%) have no mobile presence.

The majority of respondents from Indonesia (66.7%) and the Philippines (64.5%) have not yet taken up mobile. There are more merchants in the Philippines who have a mobile site (9.7%) than in Indonesia (6.7%). But merchants with an app (16.7%) or both (10%) in Indonesia surpassed those in the Philippines (app, 16.1%; both 9.7%).

2.4%

Mobile Fraud Rate

1 IN 3 OR 37.5% OF MERCHANTS DO NOT KNOW THEIR MOBILE FRAUD RATE

Close to two in three (62.5%) survey respondents said they know what their mobile fraud rate is, underscoring the presence—and impact—of mobile fraud in SEA.

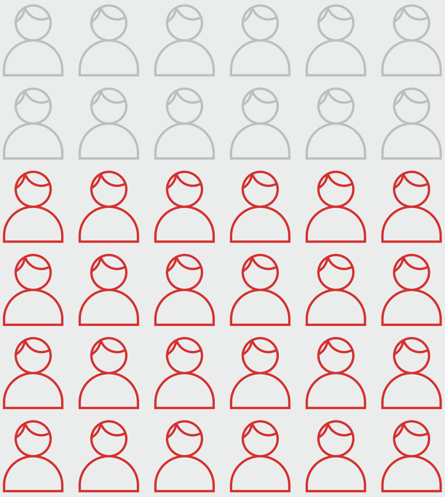
Respondents on average lost 2.4% of their revenue to mobile fraud, according to those affected. Incidentally the survey saw that the number of merchants aware of their mobile fraud rate was inversely proportional to the amount of revenue lost. To wit, 90% of Singapore respondents know their mobile fraud rate, and tracked their revenue losses to be at 1.2%. In contrast, only 45.2% of the Philippines respondents know their mobile fraud rate, which lost them 3.5% of their revenue.

In Malaysia, 71% of merchants know their mobile fraud rate that caused to lose 2.1% of their revenue. Thailand and Indonesia each had 53.3% of merchants who know what their mobile fraud rate is, except Thailand's mobile revenue fraud loss (2.9%) was lower than Indonesia's (3.3%).

Considering the survey previously found Singapore and Malaysia to have the most mobile presence, the results here may be attributed to unfamiliarity or inexperience in handling mobile fraud, which has its differences from online fraud. Merchants have to bear these distinctions in mind when managing cross-channel fraud, especially for markets where mobile broadband penetration is rising faster than fixed broadband.

3 IN 4

Merchants Do Not Screen Mobile Fraud



MOBILE FRAUD RISKS DIFFER FROM ECOMMERCE FRAUD RISKS

Consumer use of mobile platforms to shop and pay online is catching on in SEA, which will eventually pave the way for mobile to become a key revenue channel for online merchants—as well as a keen target of fraudsters looking for new or unknown gaps to exploit.

Three in four respondents (75%) in the survey, however, said they currently do not screen for mobile fraud. This corroborates with the region's current sporadic mCommerce adoption. But it may also reflect sentiments that the platform is too difficult or inconsequential at the moment to warrant tracking. Respondents who have less eCommerce revenue and experience—the Philippines (93.5%), Thailand (83.3%) and Indonesia (83.3%)—formed the majority in this group, as opposed to Malaysia (67.7%) and Singapore (46.7%).

For the quarter of respondents who do screen mobile fraud, they use different tools (15.8%) rather than eCommerce tools (9.2%)—an approach seen across all five countries. A consideration of the differences of fraud risks present in eCommerce and mCommerce channels is a step in the right direction, because applying eCommerce screening tools for mobile could lead to fraud screening that is too lax or too rigid, affecting not only the mobile fraud rate, but the mobile order acceptance rate too.

91.5%

Feel Mobile Fraud Riskier Than Online Fraud

FEW BELIEVE MOBILE CHANNEL IS LOW RISK

A whopping 91.5% of respondents believe mobile fraud to be risker than online fraud—further classified as “somewhat higher risk” (53.3%), and cited “significantly higher risk” (38.2%)—which puts an ironic spin to the previous finding that 75% of them do not screen mobile fraud. Only a handful of respondents felt there is “no difference” (6.6%) or “somewhat lower risk” (2%).

All the countries shared similar outcomes. Starting with Thailand, two thirds of merchants called mobile fraud “somewhat higher risk” (60%) and half that number said “significantly higher risk” (33.3%). Next was the Philippines, “somewhat higher risk” (54.8%) and “significantly higher risk” (35.5%); then Indonesia, “somewhat higher risk” (53.3%) and “significantly higher risk” (40%).

In Malaysia the gap between the “somewhat higher risk” (51.6%) and “significantly higher risk” (41.9%) camps narrowed, as with Singapore, “somewhat higher risk” (46.7%) and “significantly higher risk” (40%). Singapore also had the most number of merchants (13.3%) who believed there is “no difference” between mCommerce and eCommerce fraud risks.

Because of the smaller form factor and real estate space on mobile devices, online shopping behaviour, consumer expectations and the underlying technology are also different from traditional PCs and laptops. Fraudsters may exploit these differences that the mobile channel holds, so merchants must account for them, even if they are very experienced in mitigating eCommerce fraud. Otherwise fraudulent orders on mobile may slip past them unnoticed, or valid orders get mistakenly rejected. Either scenario spells out revenue losses that could have been avoided.

ABOUT
CYBERSOURCE

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 475,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in Foster City, CA and maintains offices throughout the world, with regional headquarters in Singapore, Tokyo, Miami/Sao Paulo and Reading, U.K.

For more information, please visit
http://www.cybersource.com/asiapacific

CONCLUSION

What this report has unearthed is merchants in the five SEA countries need to overcome fraud with the right tools and the right approach on how to manage it. The high false positive rate and confidence of 3-D Secure as a sufficient fraud protection strategy are two examples of how mindsets can either diminish or drive revenue in a region where there are massive growth opportunities in online and mobile commerce.

To capture the potential for more revenue and customers in a market as diverse as SEA will require effective fraud management practices. This report is just part of CyberSource's ongoing efforts to educate merchants in understanding the key aspects of payment fraud management as both business and fraud risks evolve.

CyberSource is the leading payments and fraud management provider, with our Decision Manager fraud detection platform, Decision Manager Replay real-time fraud analysis tool, and Managed Risk Services for global fraud risk expertise, just to name a few. We are your trusted partner to help you work your way through the entire journey to enable strategy , solutions and success in fraud management and most of all, your business ambitions.

DISCLAIMER

Case studies, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. You should consult with your legal counsel to determine what laws and regulations may apply to your circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

CONTACT US:

ASIA PACIFIC

t. **001-800-6671-5000** (Singapore/Thailand)
t. **00-800-6671-5000** (Malaysia)
t. **000-800-630-1003** (India)
t. **1-800-8-756-8388** (Philippines - Globe)
t. **1-800-10-80v2-7222** (Philippines - PLDT)
e. **ap_enquiries@cybersource.com**

Greater China
e. **gc_enquiries@cybersource.com**

Australia & New Zealand
t. **0011-800-6671-5000** (Australia)
t. **00-800-6671-5000** (New Zealand)
e. **anz_enquiries@cybersource.com**

JAPAN

Tokyo, Japan
t. **+81 3 3548 9873**
e. **sales@cybersource.co.jp**

EUROPE, MIDDLE EAST & AFRICA

Reading, United Kingdom
e. **europe@cybersource.com**

LATIN AMERICA & THE CARIBBEAN

Miami, FL, United States
e. **lac@cybersource.com**

Mexico
e. **mexico@cybersource.com**

Brazil
e. brasil@cybersource.com

NORTH AMERICA

Foster City, CA, United States
e. **sales@cybersource.com**

www.cybersource.com/asiapacific