Acquirer PCI Sentiment Survey

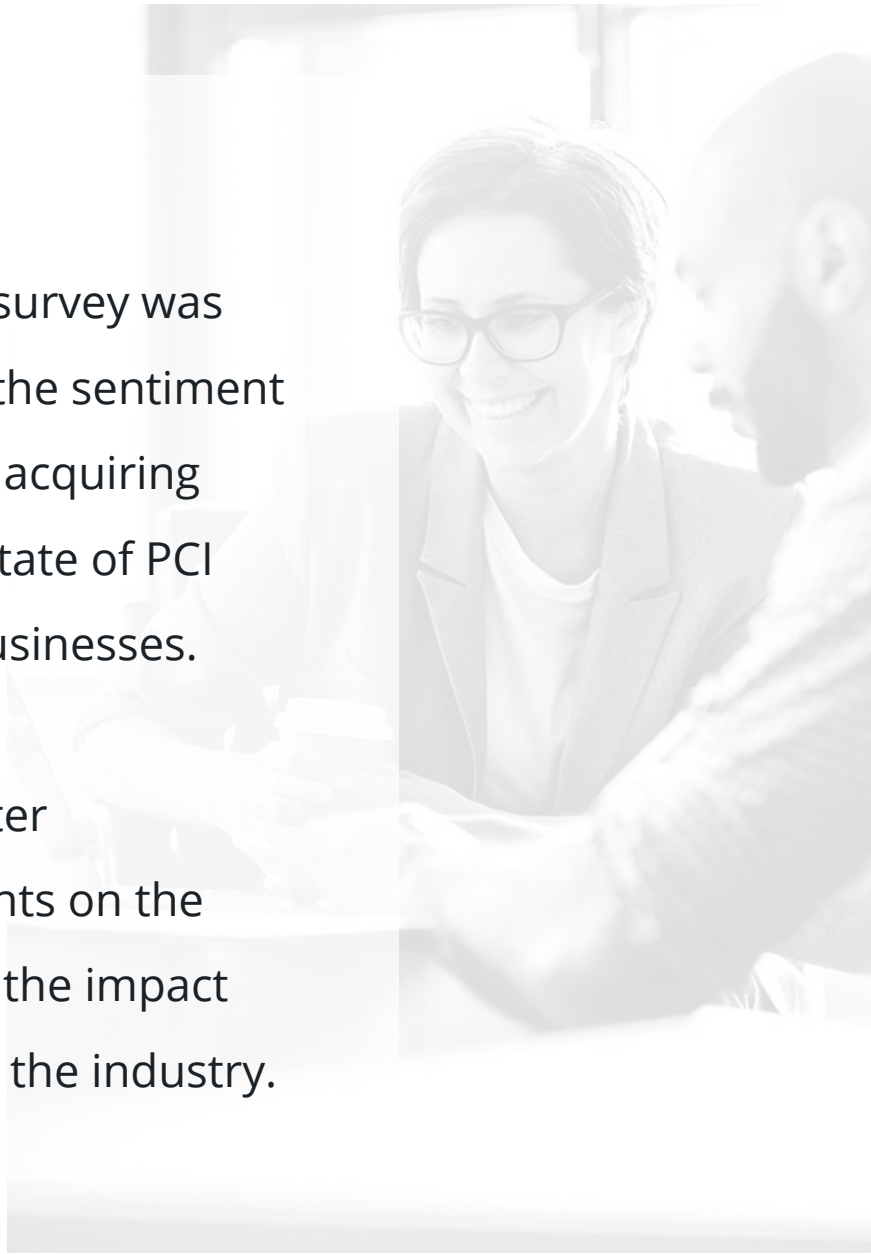
Sentiment Survey | April 2018

Senior payment executives' thoughts on SME PCI compliance and security

sysnet global solutions

What the future holds for the PCI DSS and the impact of non-compliance fees

Sentiment Survey | April 2018



Introduction

The inaugural PCI Sentiment survey was conducted in order to gauge the sentiment of senior executives at global acquiring organisations regarding the state of PCI compliance amongst small businesses.

We also wanted to gain a better understanding of their thoughts on the future of the PCI DSS, and on the impact non-compliance fees have on the industry.

Welcome Message

We conducted this survey to put some structure on the many conversations we have had with acquiring organisations who feel that they are fighting a losing battle when it comes to getting and keeping smaller businesses secure and compliant.

At Sysnet, we constantly strive to **make the compliance journey as easy as possible** for merchants, but we also want to **make a real impact on their security**. The survey results have strengthened our resolve to remove the burden of compliance and security management for all small businesses.

We are very grateful to all those who responded to the survey and are pleased to share the findings with them and the broader acquiring industry.

We hope the results will enable the industry to change the current approach to compliance and security for smaller businesses and, in doing so, help those businesses to survive and thrive in an increasingly complex cyber security environment.

Gabriel Moynagh
Chief Executive Officer, **Sysnet Global Solutions**

5 key takeaways from the PCI Sentiment Survey

1. **All acquirers agree that small merchants are not effectively engaging with PCI programs**: the majority believe that this is a result of a lack of knowledge and time.

2. **Less than 10% of acquirers are happy with their current compliance rate**: 96% want it to be higher than 50%, 84% want it to be greater than 70%.

3. **Over 70% of acquirers believe that the best ways to drive PCI compliance are**: regular communication, merchant education and the provision of managed security and compliance services.

4. **Almost 80% of respondents agree that PCI non-compliance fees should not be charged for any longer than 24 months**: 21% feel it is never appropriate to charge non-compliance fees.

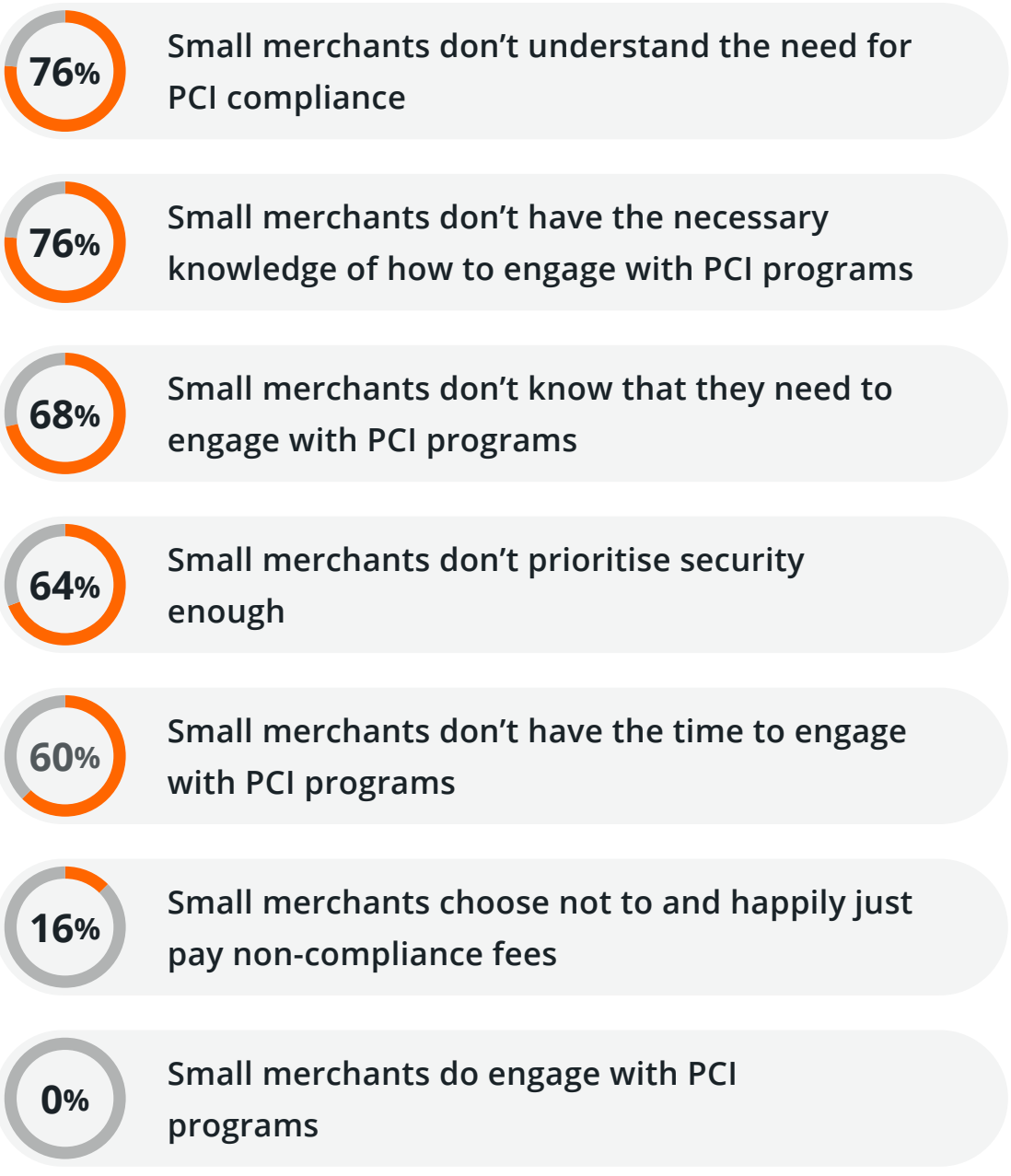
5. **96% of respondents agree that acquirers need to do more to help merchants secure their businesses.**

Survey Findings

Q Why do you think small merchants do not engage with PCI programs?

There is an overwhelming response from acquirers who feel **merchants do not effectively engage with compliance programs.**

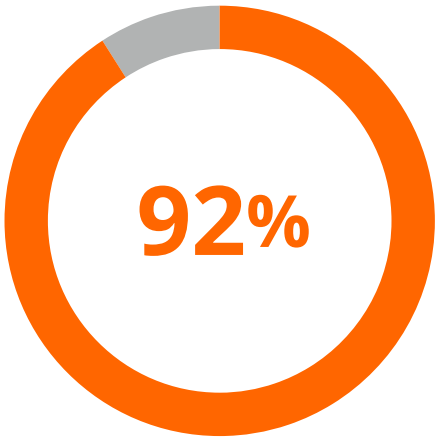
Very few acquirers feel that merchants simply choose not to engage. **Most agree** that merchants either **don't know they need to**, **don't understand what they need to do** or simply **don't have the time or knowledge needed**. Many also feel that merchants don't prioritise security.



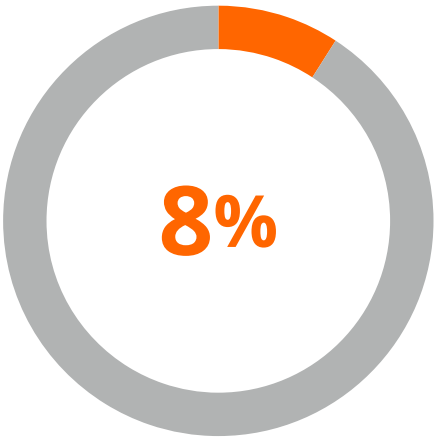
Q Are you comfortable with your current PCI program compliance rate, or would you like it to be higher?

The **vast majority** of respondents indicated that they are **not happy with their current PCI program compliance rate**, and **only 8%** indicated that they **are happy** with their current PCI program compliance rate.

92% of respondents are not happy with their current PCI program compliance rate.



I would like our compliance rate to be higher

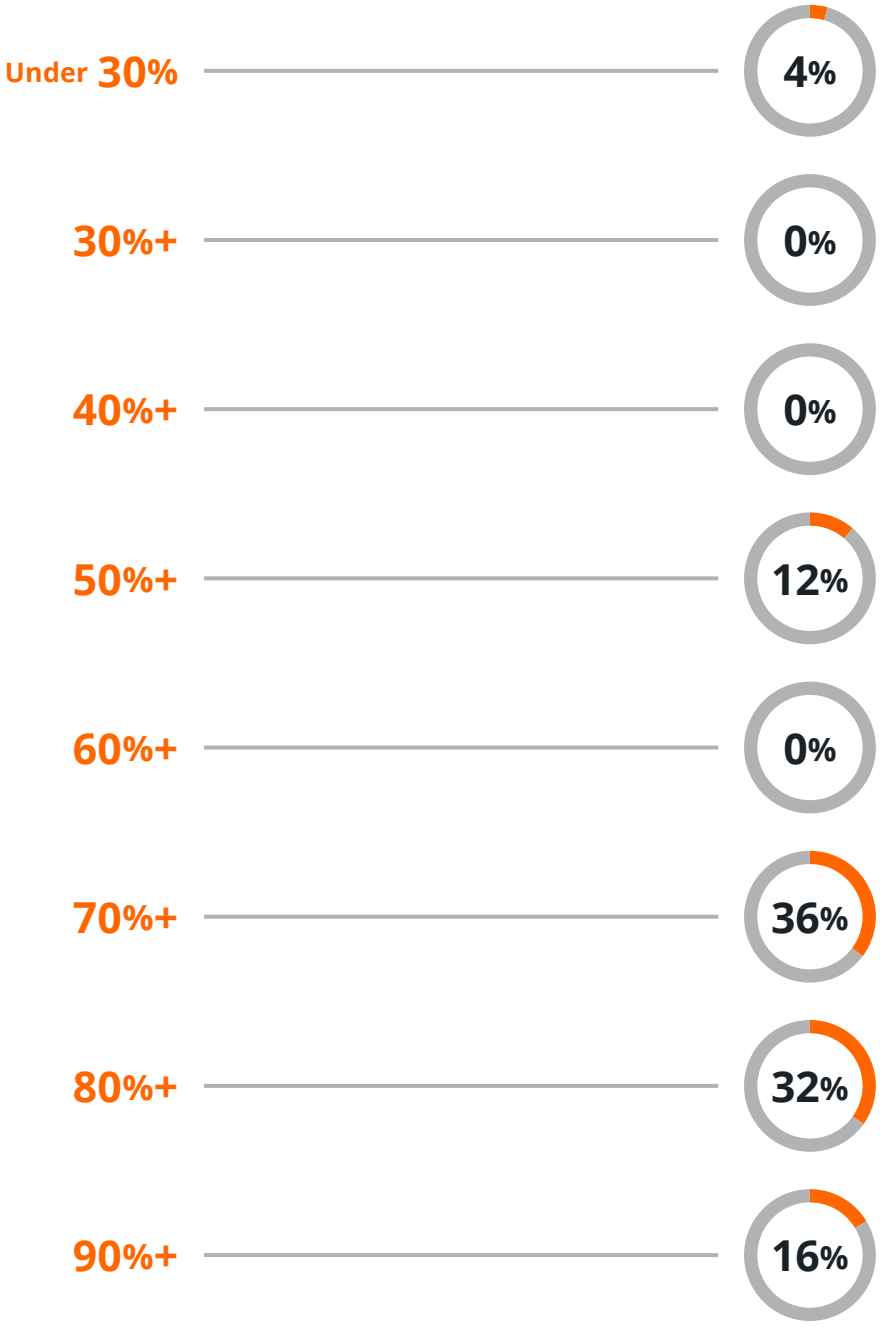


I am comfortable with the current rate

What do you believe to be an acceptable compliance rate?

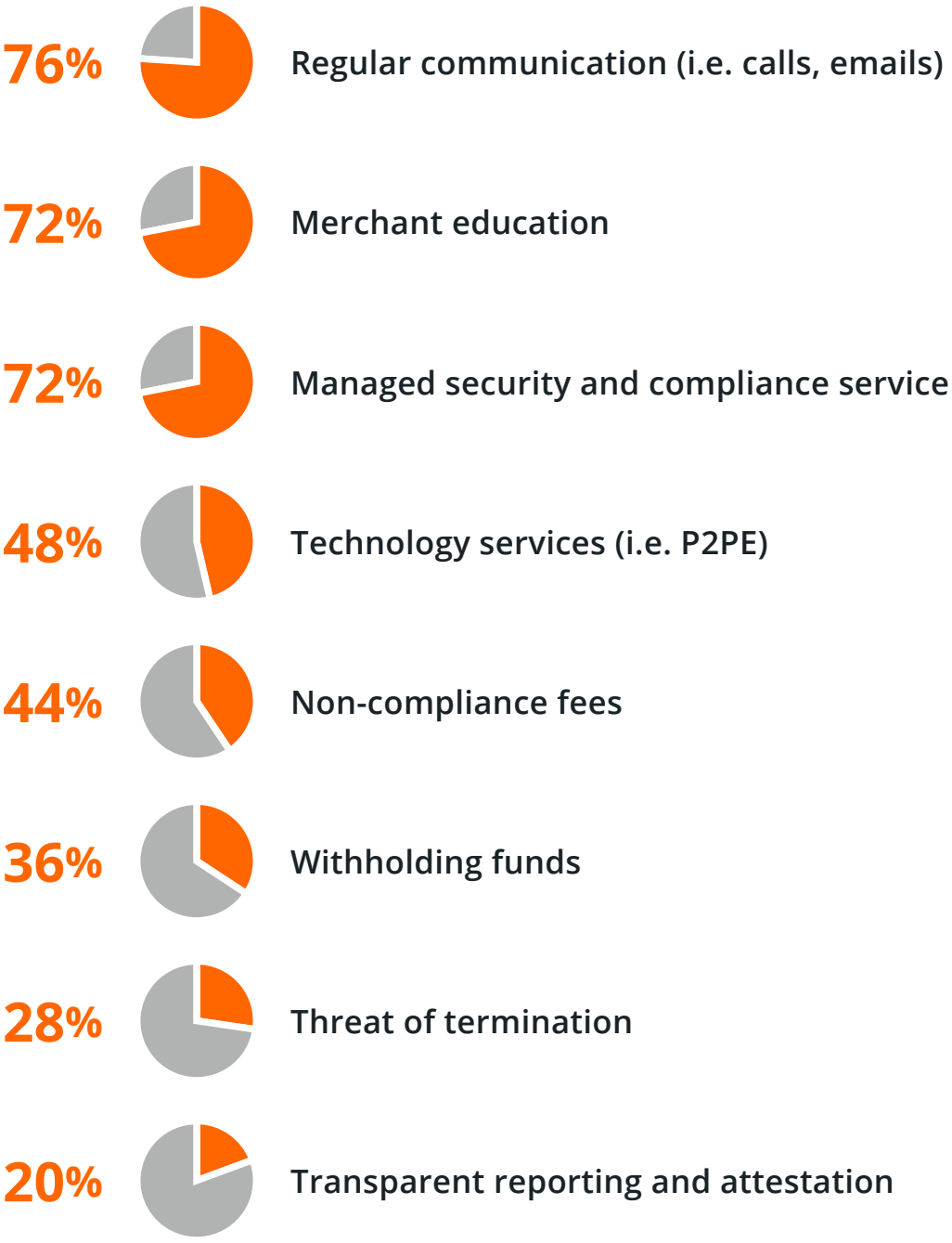
96% of respondents would like their PCI program compliance rate to be higher than 50%.

A **very small minority of just 4%** would be happy with a compliance rate of **under 30%**. **84%** would like their compliance rate to be **greater than 70%**, while **16%** desire **90% and upwards**.



Q Which of the following initiatives do you believe drives compliance?

Most respondents feel that regular communications, merchant education and the provision of managed security and compliance services **drive compliance amongst smaller merchants**.



Less effective ways of driving compliance are non-compliance fees, withholding funds, threat of termination and transparent reporting and attestation.

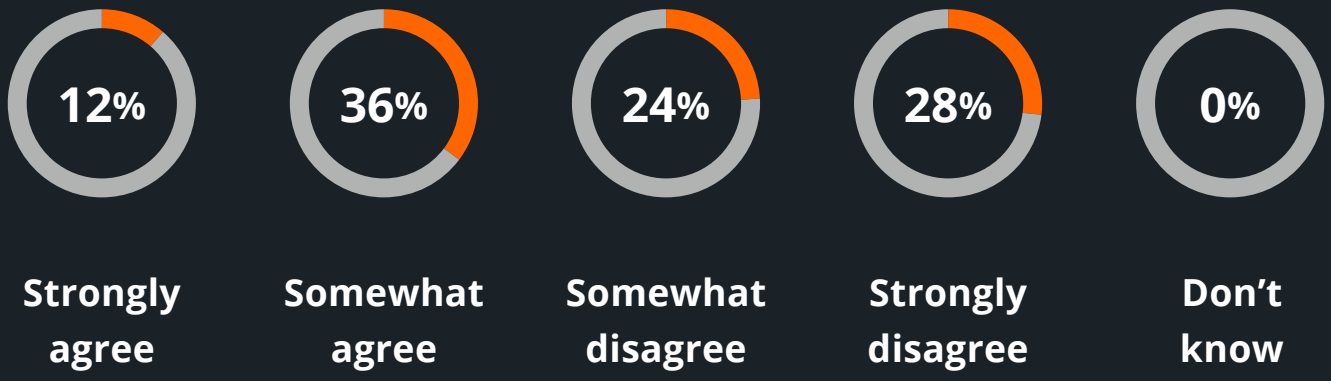
Q "PCI DSS does enough to ensure a small business is protected from cyber attacks."

To what extent do you agree or disagree with this statement?

Less than half of the respondents **agree** with this statement.

One respondent commented that if PCI DSS is all they do, they are a lot better off than doing nothing at all.

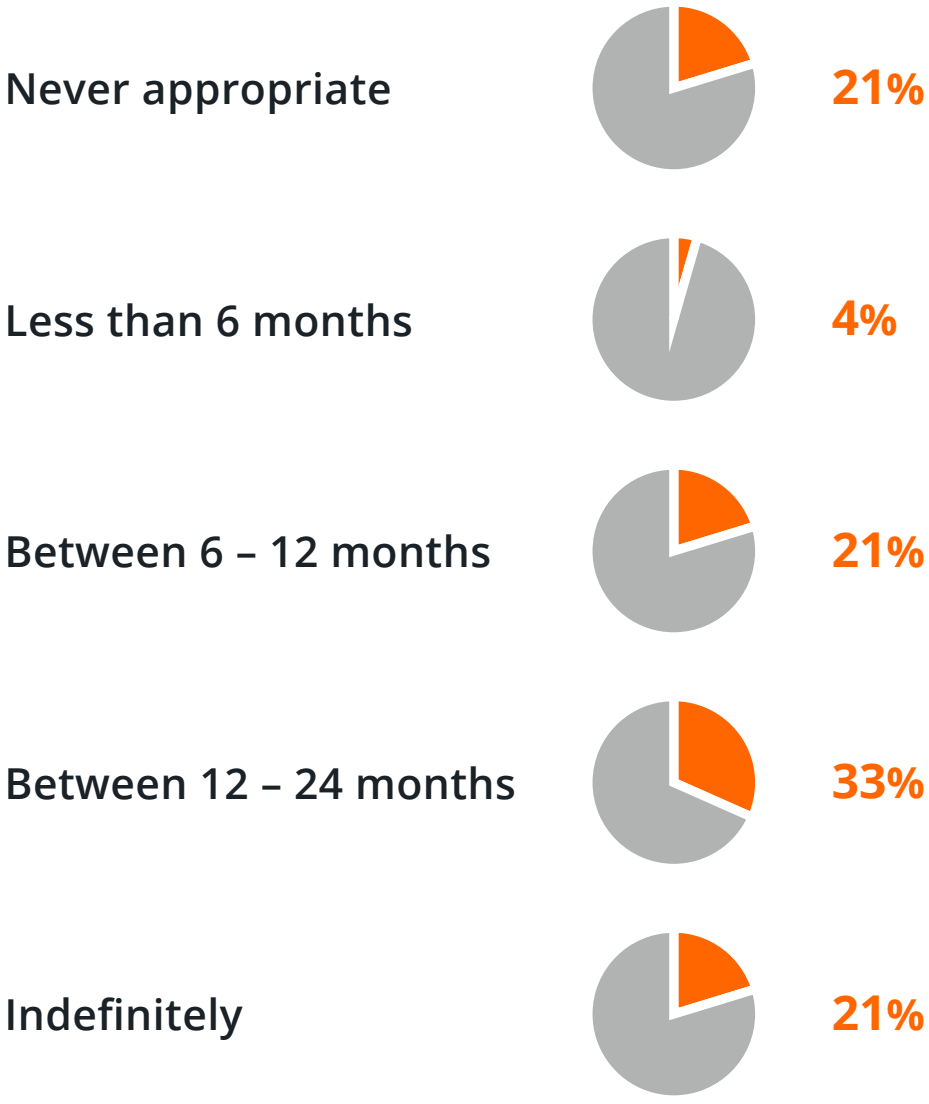
Over 50% of respondents **somewhat or strongly disagree** with the statement that the PCI DSS does enough to ensure a small business is protected from cyber attacks.



Some feel that PCI DSS **does not drive good practices** and **behaviours for small merchants**, while others believe that it only provides the tool to use to defend against cyber attacks.

Q For how long do you think it is appropriate to charge a small business non-compliance fees before taking alternative action?

Almost 80% of respondents agree that PCI non-compliance fees **should not be charged** for **any longer than 24 months**.



21% of respondents feel it is **never appropriate** to charge non-compliance fees.

One respondent commented that security is part of a service that payment providers should be offering to customers, and not using the excuse of non-compliance as a revenue generator.

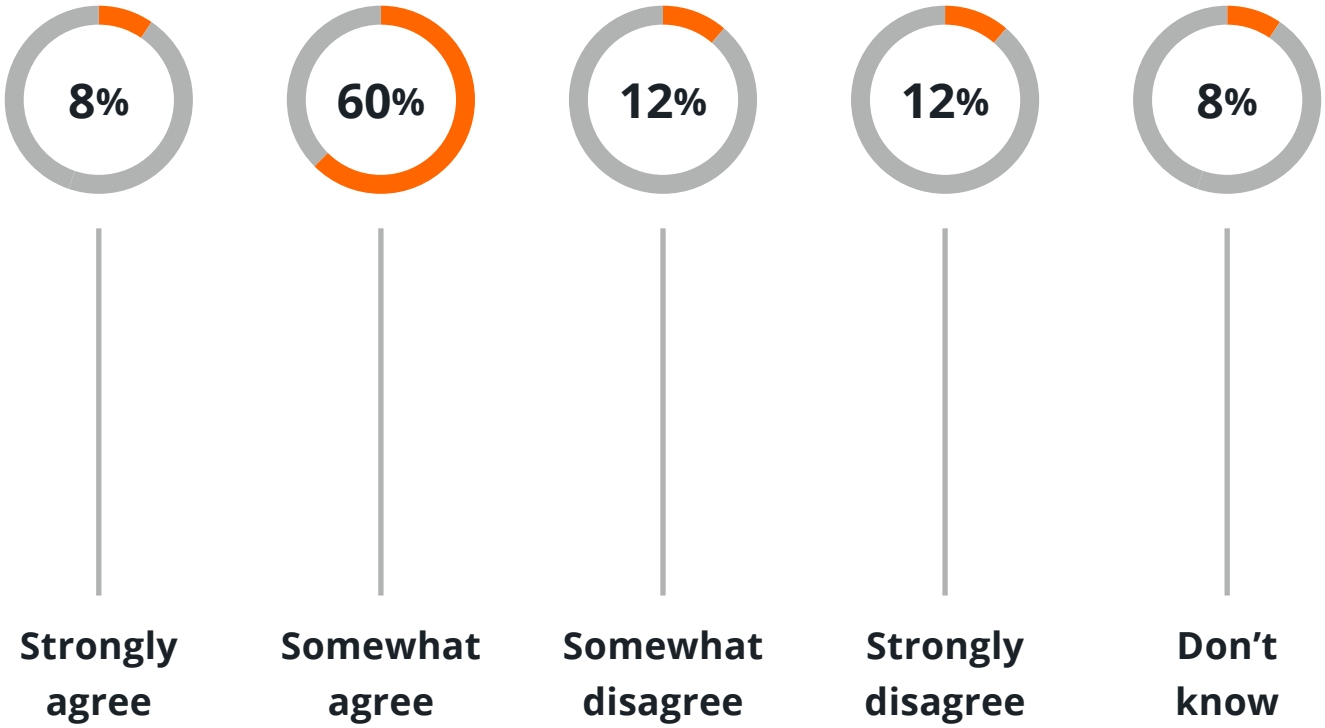
Q "It is likely that some form of regulation will be introduced to control PCI charges in the future."

To what extent do you agree or disagree with this statement?

68% of respondents **agree** that it is likely that some form of **regulation will be introduced** to control PCI charges in the future.

One respondent commented that they felt it will be considered in a similar category as PPI or other forms of 'insurance'. Another respondent also commented that, although it is somewhat likely, merchants will need to be given ample notice.

Only **24% disagree.**



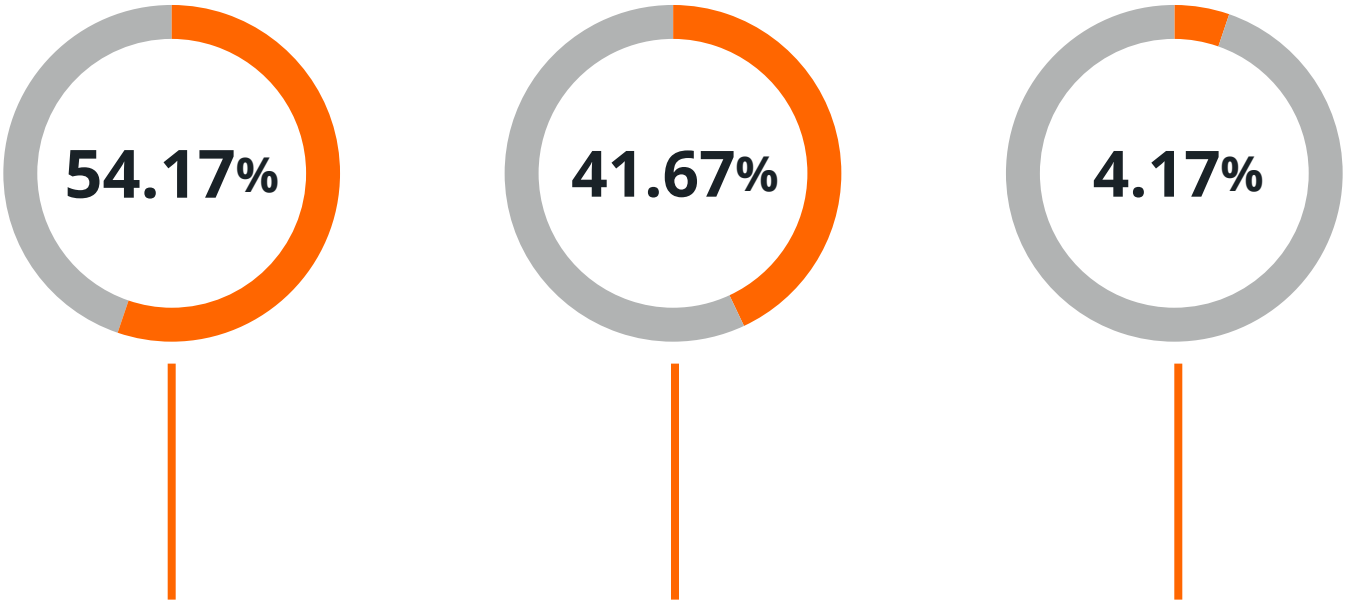
Q Have you considered providing cyber security tools to your small business merchants?

(e.g. tools such as P2PE that reduce PCI scope.)

54% of respondents are already **providing cyber security tools** to their small business, which include PCI scope reducing tools like point-to-point encryption tools.

42% are currently **considering providing such tools**, with some trying to understand the real business benefit to customers versus the costs.

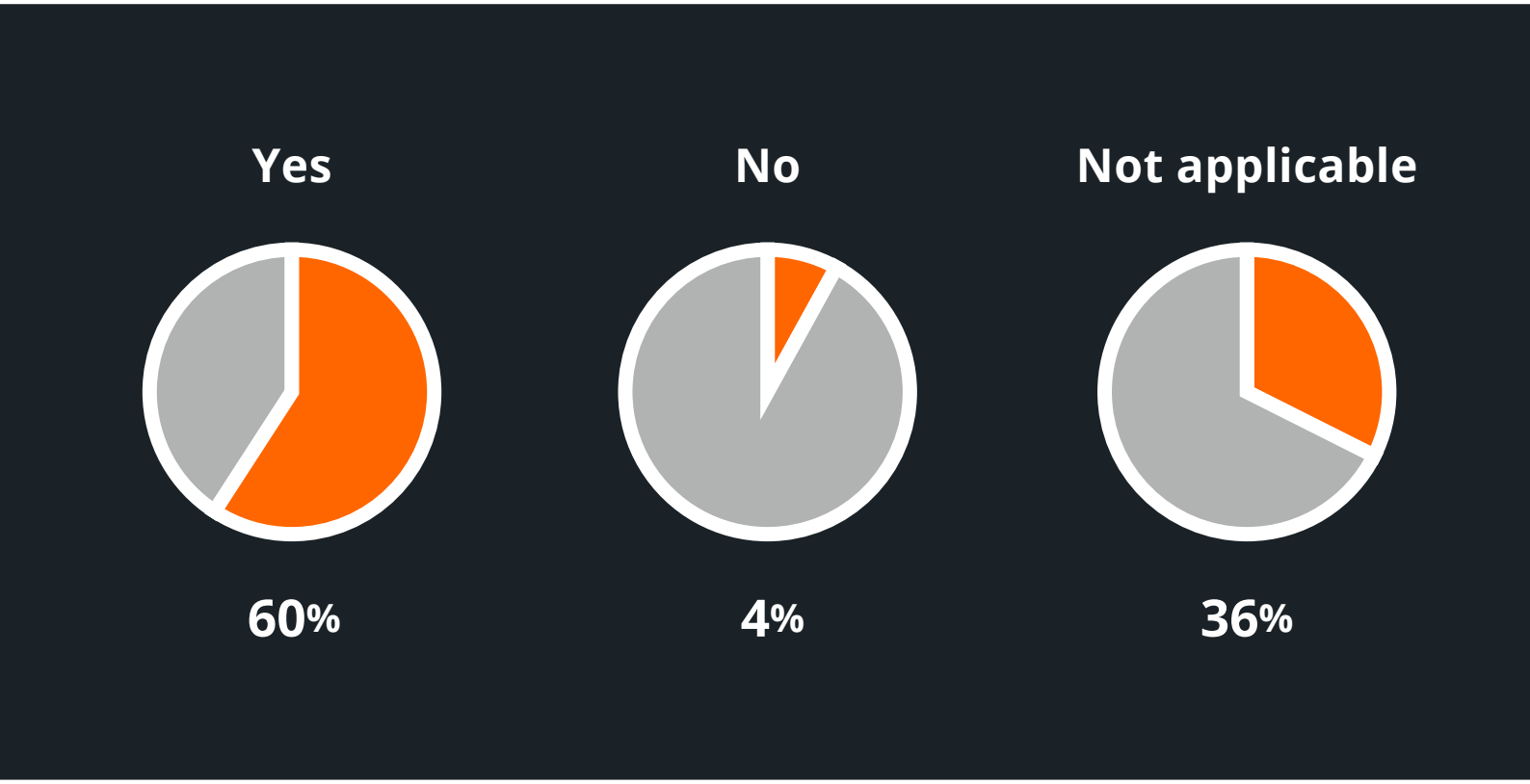
Just **4%** have considered providing them but decided not to.



Q If you are currently providing managed compliance and security services to part of your merchant portfolio, do you plan to extend this to more of your merchants in the future?

64% of respondents indicated that they are **currently providing managed compliance** and **security services** to part of their merchant portfolio.

Of those who are currently providing managed services to part of their merchant portfolio, **94% indicated** that they plan to **extend this service** to more of their merchants in the future.

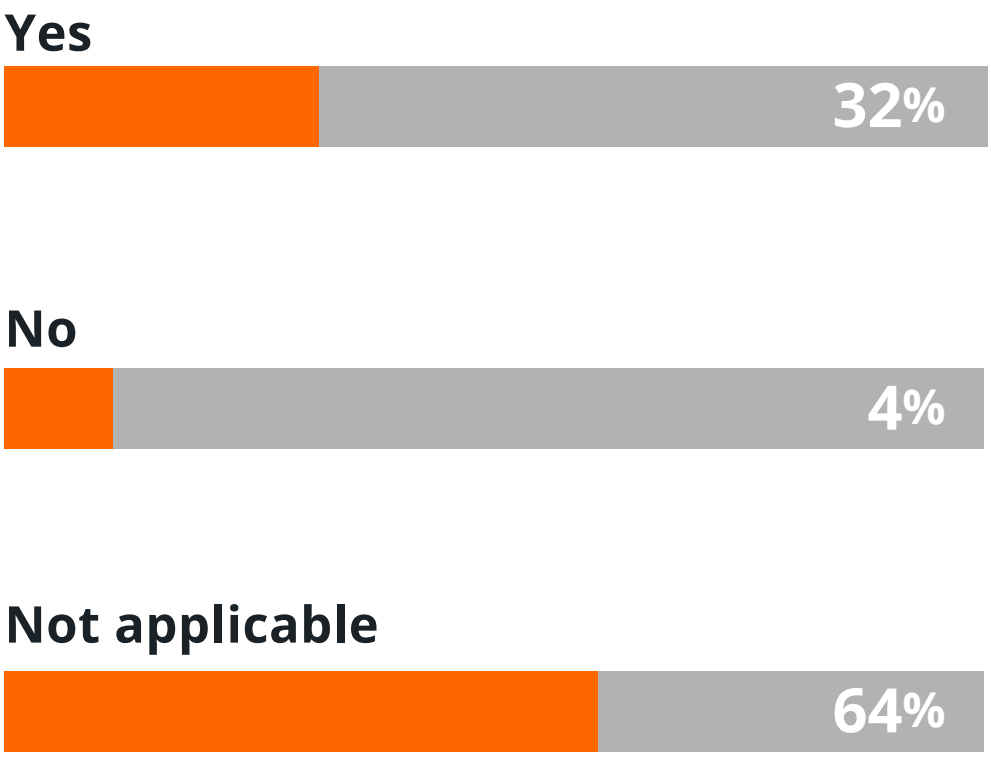


Only 6% of those currently providing, **do not plan to extend their managed compliance** and **security services** to more of their merchants in the future.

Q If you do not currently provide managed compliance and security services, would you consider providing it in the future?

Of the **36% of respondents** who **do not currently provide managed compliance** and **security services** to their merchant portfolio, **89%** would consider doing so in the future.

Only 11% of those **not currently providing managed compliance** and **security services** would not consider doing so in the future.

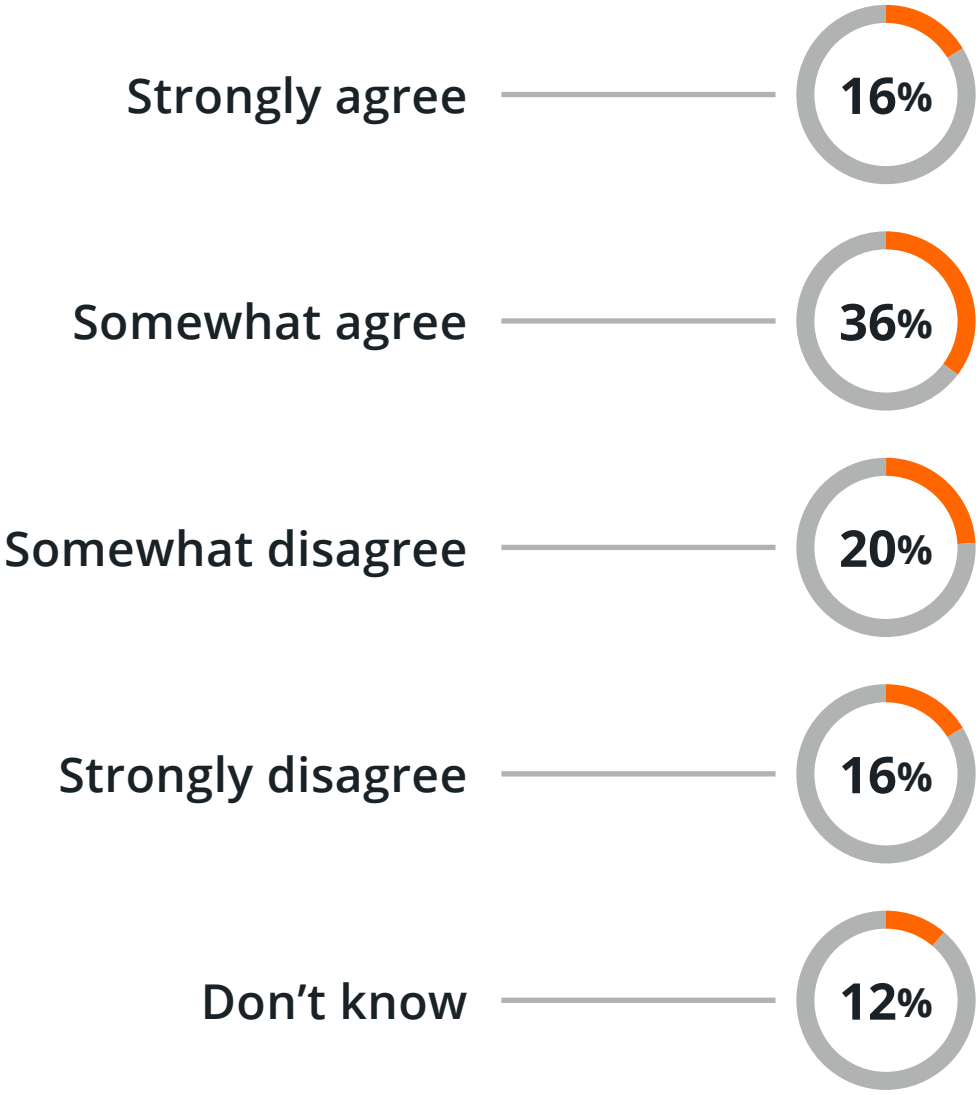


Q Some acquirers view non-compliance fees as unethical, describing PCI non-compliance fee revenue as ‘a drug the industry needs to wean itself off’.

To what extent do you agree or disagree with this viewpoint?

52% of respondents agree with this statement.

One respondent commented that it is taking advantage of customers by forcing them to pay extra fees and carry all the risks associated with non-compliance. Another commented that, while they agree, it is up to industry officials to lead change.



36% of respondents disagree with this statement.

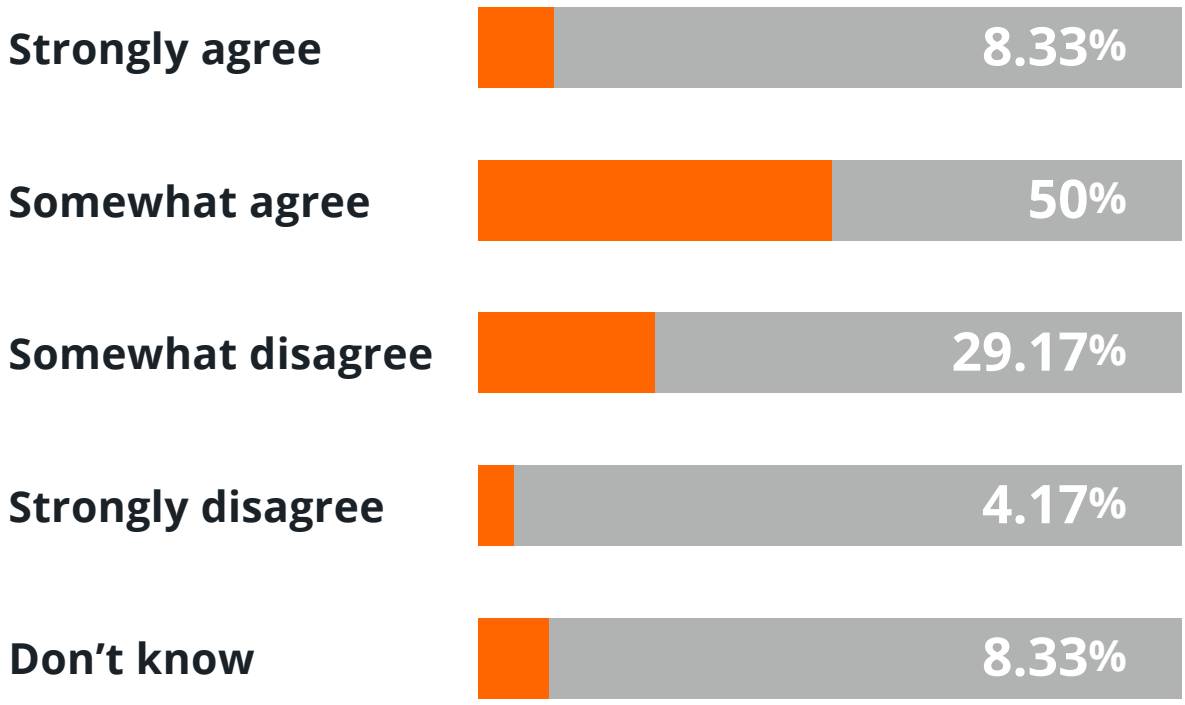
Some who disagree feel it is up to every regulated entity to ensure that they treat customers fairly. Others feel ‘unethical’ is a strong statement, even though they don’t like them and would rather have a value added fee than a non-value added fee.

“Non-compliance fees contribute to merchant attrition.”

To what extent do you agree or disagree with this statement?

Over 58% agree that non-compliance fees contribute to merchant attrition.

One respondent commented that some merchants pay the fees rather than carry out the attestation, and some acquirers consider this a revenue stream rather than a tool to encourage attestation. Another respondent indicated that it causes friction with customers who do not understand PCI and clearly see it as a non-value cost.



Less than 34% disagree.

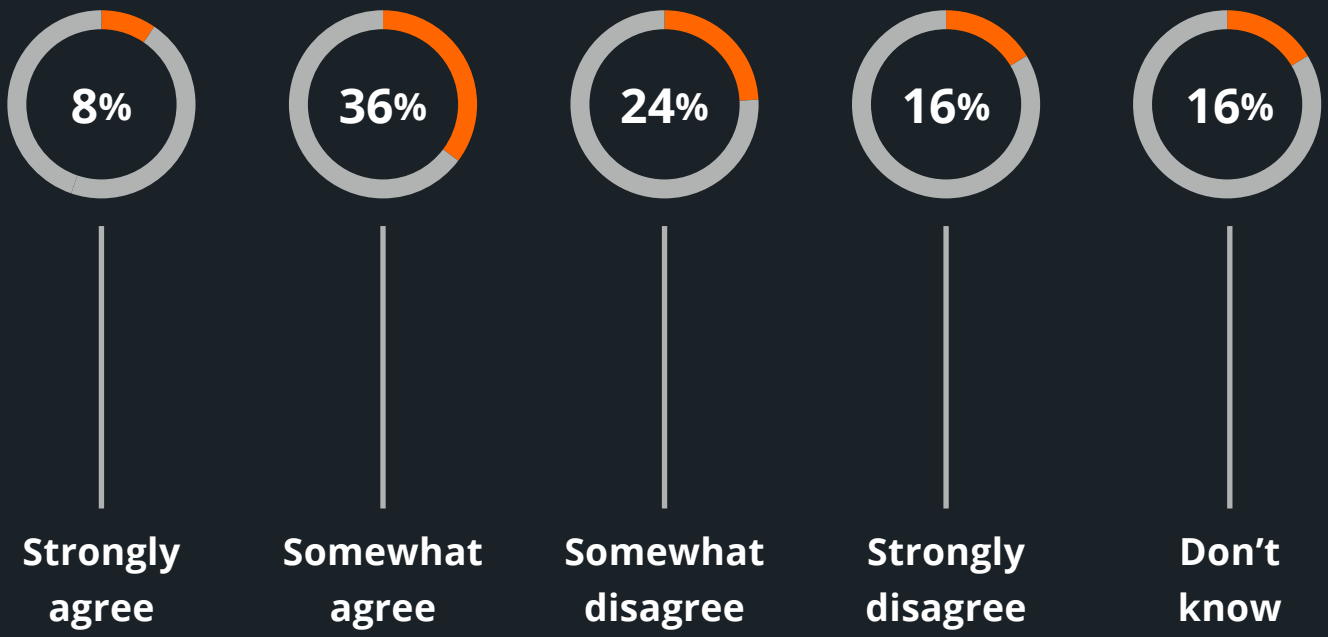
One respondent commented that they don’t think it causes much attrition as most acquirers charge the fee, so no matter where the merchant goes they are going to have to pay the fee.

Q “Charging non-compliance fees damages acquirers’ brand.”

To what extent do you agree or disagree with this statement?

44% agree that charging non-compliance fees **damages acquirers’ brand**.

40% disagree. One respondent commented that most acquirers do charge so it has become the standard.



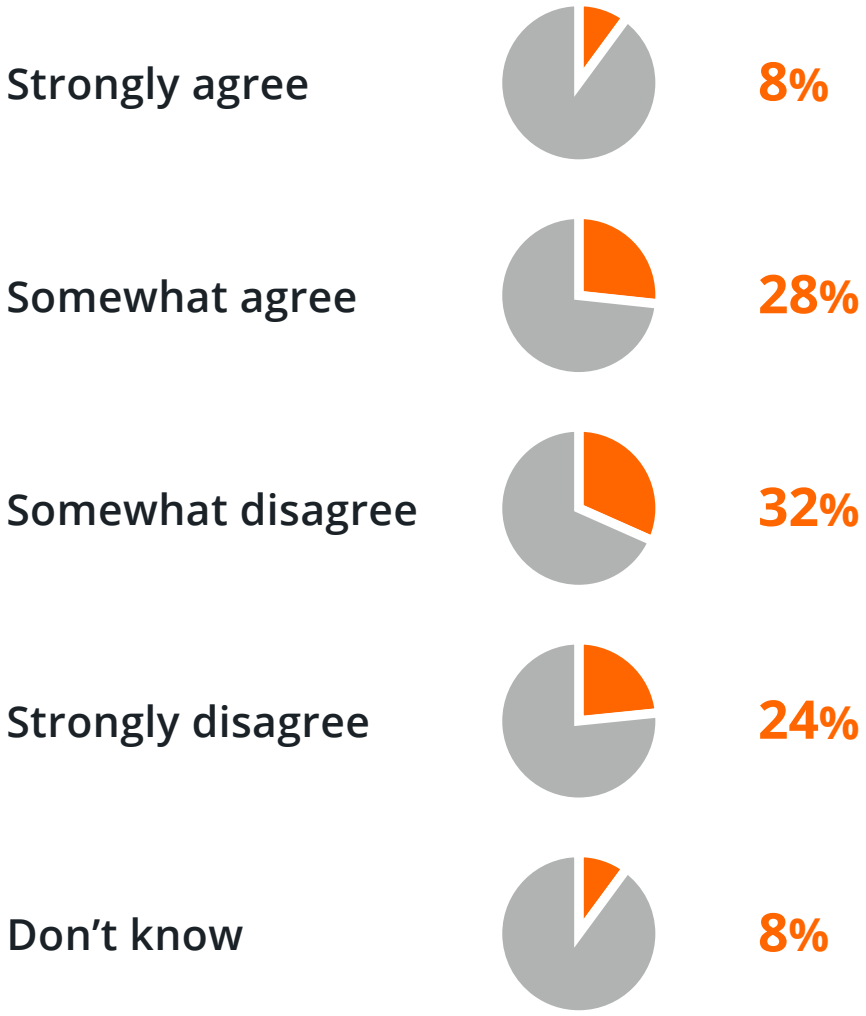
“PCI DSS, in its current format, will still be relevant in 5 years’ time.”

To what extent do you agree or disagree with this statement?

Just 36% agree that the current form of PCI DSS will still be relevant in the future, while 56% disagree.

One respondent commented that, while PCI DSS has achieved what it set out to (bringing attention to data security), the industry needs to do more to move the onus towards technology to enable compliance.

Another respondent commented that the evolving payments market and underpinning technology will bring advances that will make security breaches more difficult, however, they also felt that protection of non-payment personal data will become a bigger issue.

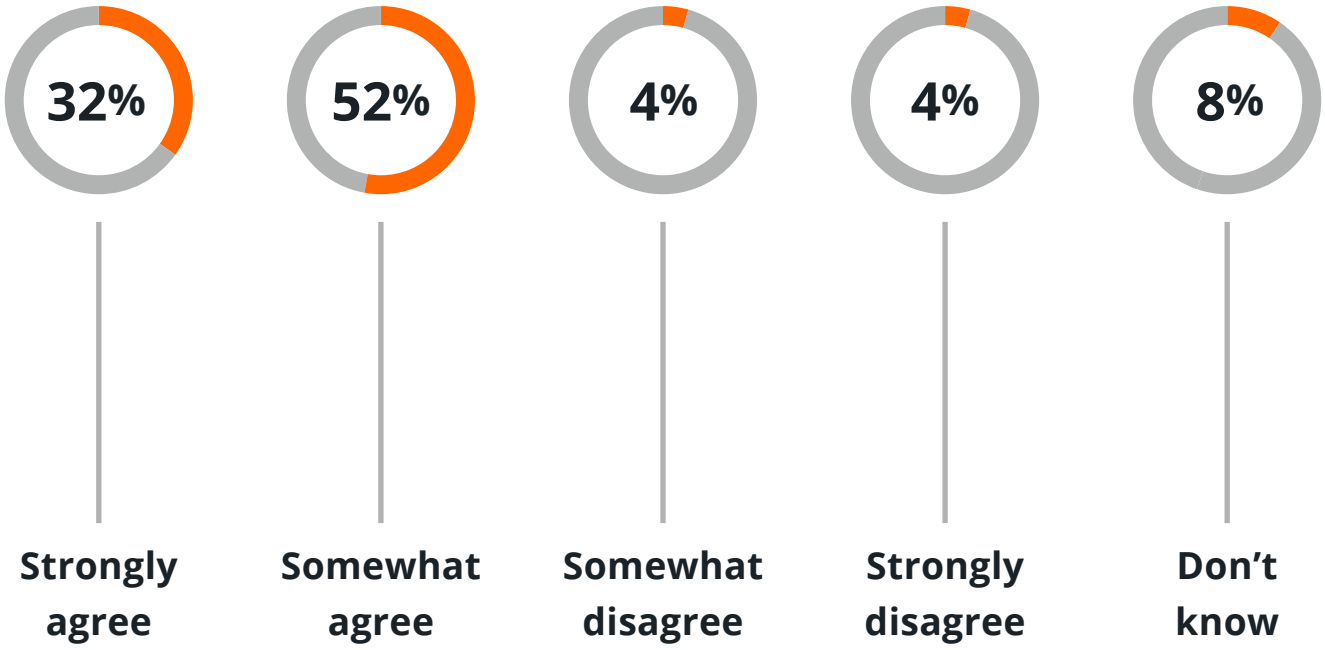


“Acquirers need to do more to help their merchants comply with PCI DSS.”

To what extent do you agree or disagree with this statement?

The vast majority, 84% agree that acquirers need to do more to help their merchants comply with PCI DSS.

One respondent commented that PCI programs have evolved in the last 10 years, with acquirers slowly adjusting their programs to aid merchants’ understanding and equip them with more meaningful information, but that they need to continue to improve and are doing so through technology and services.



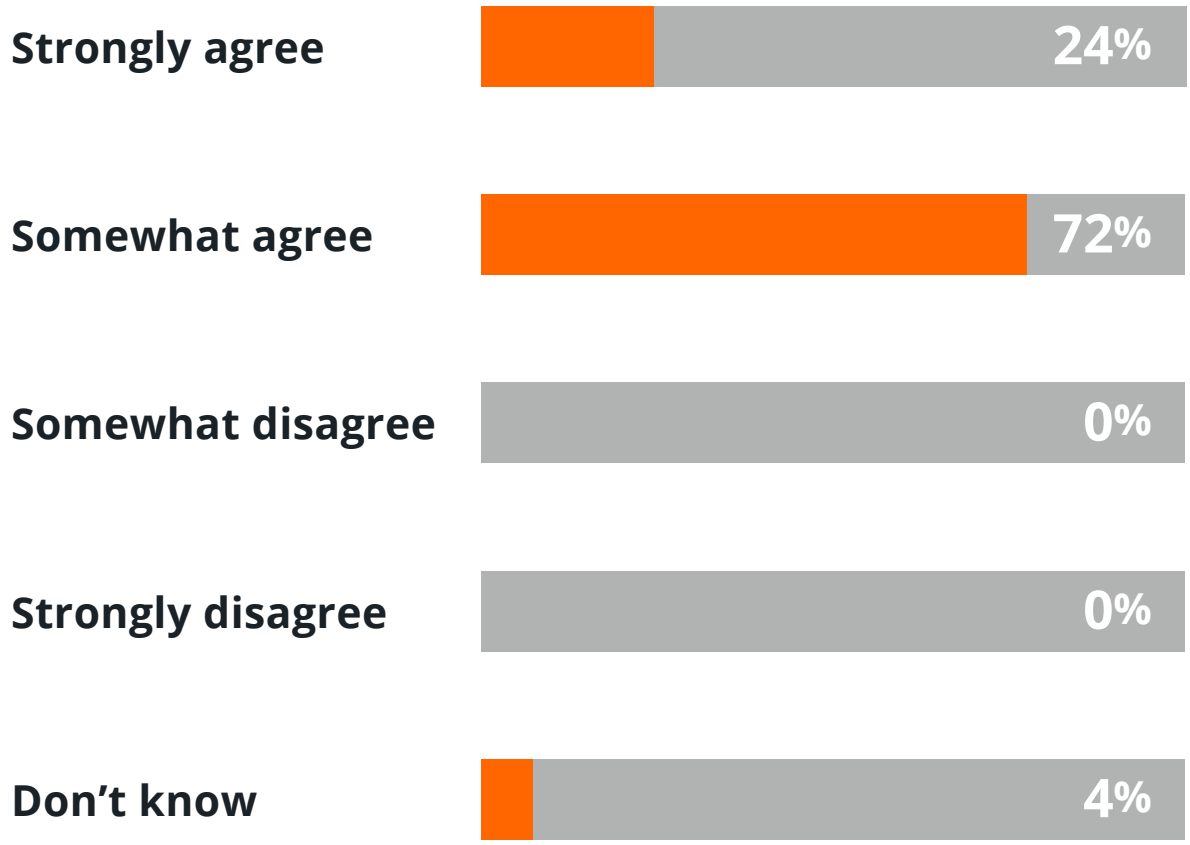
Just 8% disagree. One respondent advised they feel the acquirer’s role is to educate and support merchants in the running of their businesses.

Q “Acquirers need to do more to help their merchants secure their businesses.”

To what extent do you agree or disagree with this statement?

An overwhelming 96% of respondents agree that acquirers need to do more to help their merchants secure their businesses.

One respondent commented that acquirers have a responsibility to help customers be successful and be protected against unnecessary risks, but customers need to take responsibility for the protection of their businesses.



Recommendations

1. The key to driving successful PCI programs is to **communicate often with merchants**, educate them on the **benefits of securing their business** and, if possible, provide them with **managed compliance and security solutions** that take the heavy lifting out of compliance and security for smaller businesses.

2. Non-compliance fees are **not an effective method** of driving PCI program engagement but, if you do charge non-compliance fees, consider taking **alternative actions** within a relatively short period of time. The survey indicates that up to 24 months is generally acceptable, however, if an alternative option is available we recommend implementing it within 6 months.

3. Where possible, offer **scope reducing tools to help merchants achieve compliance more easily**.

4. Provide smaller businesses with **managed compliance and security services** that remove the burden of understanding what is applicable to a particular business environment.

“

It is likely that PCI compliance **will continue to evolve over the next five years** and it’s important for us to continue to evolve and grow our SME offering by adding new value to our payment solutions.

Working with **Sysnet**, we are already providing our SMEs with **managed PCI compliance and cyber security tools**, eliminating the need for them to navigate the complexities of the PCI standards, or figure out which security tools are appropriate for their business.

Equally important, we are making headway in moving away from non-compliance fees as the only means to drive our compliance rates higher and are already seeing positive results.

Wally Mlynarski
Chief Product Officer at **Elavon**

”

sysnet global solutions

Survey background

The PCI Acquirer Sentiment Survey 2018 was conducted over a three-week period, from **March 8th to March 29th, 2018**.

An online survey link was distributed via email to senior contacts from over 30 acquiring organisations, the majority of whom have level 4 portfolios greater than 10,000 merchants.

The survey was completed online by a total of 25 senior payment industry professionals. Most responses were anonymous, however, some did provide their personal details enabling us to confirm that at least 5 of the top 10 global acquirers are represented in these findings.

For more information

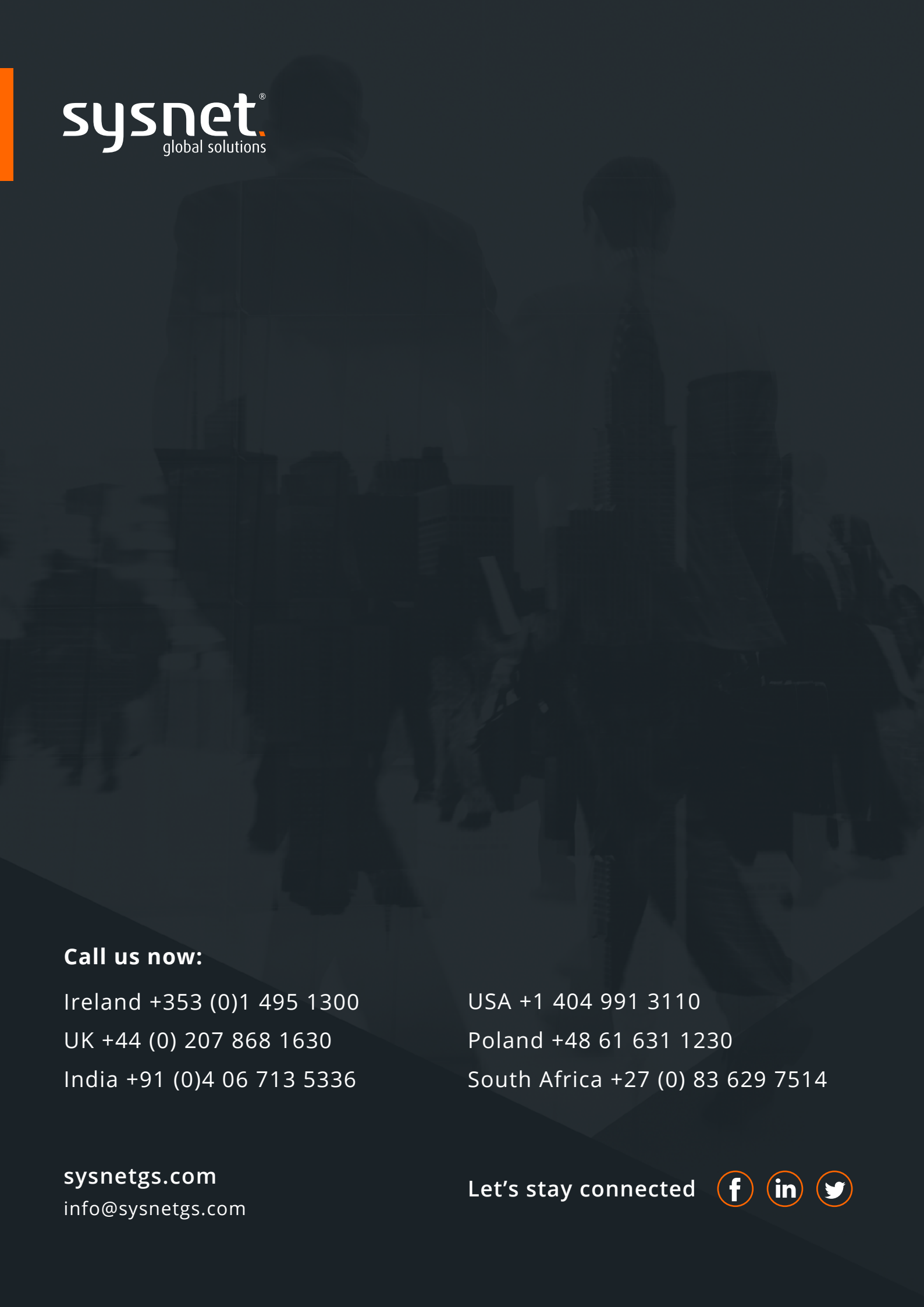
Sandra Higgins, **SVP Marketing**
sandra.higgins@sysnetgs.com

About the Survey Sponsors

Established in 1989, Sysnet Global Solutions provides payment card industry, **cyber security and compliance solutions** that help businesses to improve security and acquiring organisations to reduce risk.

Specialising in data security and PCI DSS compliance validation solutions, Sysnet offers a range of services, including its award-winning, proprietary, cyber security and compliance management solution **Sysnet.air®**, to a wide variety of businesses including acquirers, ISOs, international banks, payment service providers and merchants.

Headquartered in Dublin, Ireland, Sysnet has **clients in more than 55 countries worldwide.**



Call us now:

Ireland +353 (0)1 495 1300
UK +44 (0) 207 868 1630
India +91 (0)4 06 713 5336
USA +1 404 991 3110
Poland +48 61 631 1230
South Africa +27 (0) 83 629 7514

sysnetgs.com
info@sysnetgs.com

Let's stay connected