VikingCLOUD™

WHITEPAPER

MARCH 21, 2023 V1.1

HOW PROCESSORS CAN **INCREASE PCI COMPLIANCE REVENUE AND REDUCE ATTRITION** BY OFFERING A **MANAGED COMPLIANCE AND SECURITY SERVICE**

TABLE OF CONTENTS

Introduction 3

Non-compliance fee income – a false economy 4

Why merchant compliance matters 5

You can have your cake and eat it too 6

How do you replace non-compliance fee revenue cost-effectively? 7

The prize for high growth annual recurring revenue is big 8

Why retention matters 9

Conclusion 10

INTRODUCTION

HOW PROCESSORS CAN **INCREASE PCI COMPLIANCE REVENUE AND REDUCE ATTRITION** BY OFFERING A MANAGED COMPLIANCE AND SECURITY SERVICE

In this white paper, we discuss how processors can reduce their reliance on PCI non-compliance fee revenue while setting the stage to deliver enhanced security capabilities that increase PCI compliance, reduce merchant churn, and dramatically enhance overall recurring revenue.

We also discuss how improved merchant experience and security posture result in lower churn and increased revenue lifting the overall lifetime value (LTV) of the merchant.

INCREASE COMPLIANCE, SECURITY AND RECURRING REVENUE

NON-COMPLIANCE FEE INCOME
A FALSE ECONOMY

The vast majority of payment processors charge their level 4 merchants a PCI non-compliance fee for failure to establish PCI compliance through available self-service programs in a timely fashion. These fees typically range from $240 to $750 per merchant per year. Such fees have been around for quite a long time; however, they are now beginning to attract regulatory interest.

In the US, following recent litigation, some processors are reconsidering their approach to non- compliance fees. Rather than applying fees when merchants don't comply, they are looking to incentivize merchants to become compliant by offering discounted fees upon compliance. In the UK, the Payment Services Regulator[1] investigated a range of processing fees, including those relating to PCI programs and associated non-compliance fees. Contributors to the draft terms of reference for this publication referred to PCI programs and associated non-compliance fees that do little to make a merchant secure or assist them in the event of a breach.

Despite non-compliance fees being referred to as 'a drug the industry needs to wean itself off', there has been an understandable reluctance to do so given the significant revenue they generate. However, this practice creates a false economy. Punishing non-compliant merchants without offering a viable alternative fuels attrition. Not only does this result in the loss of recurring revenue and up/cross-sell opportunities, it also means your sales effort results in maintaining rather than growing market share.

"A DRUG THE INDUSTRY NEEDS TO WEAN ITSELF OFF"
Despite non-compliance fees being referred to as 'a drug the industry needs to wean itself off', there has been an understandable reluctance to do so given the significant revenue they generate

[1] https://www.psr.org.uk/publications/general/psr-mr18-1-2-final-terms-of-reference-market-review-into-the-supply-of-card-acquiring-services/

Rather than continuing to charge non-compliance fees and providing no value in security to the merchants, processors need to actively help merchants to secure their business by offering robust security programs. Not only is this critical to merchants' continued success, it also provides a significantly improved customer experience.

WHY MERCHANT **COMPLIANCE MATTERS**

Compliance has many benefits for both merchants and processors. For merchants, it means, at the very least, they don't have to pay unnecessary non-compliance fees. But more importantly, it also helps them to avoid the negative consequences of a data breach, including reputation damage, loss of customers/revenue, inability to trade, fines, and even the possible demise of their business. If they do survive, they will also have additional compliance requirements following the breach.

For processors, helping merchants to get and stay compliant not only enables them to meet card schemes requirements it also significantly reduces risk within their merchant portfolio. The merchant compliance process also helps processors to better understand their merchants' payment environments which can enable up-sell and cross-sell opportunities. Ultimately, it helps reduce the risk of losing the business to the consequences of a breach.

COMPLIANCE HAS MANY BENEFITS FOR **BOTH MERCHANTS AND PROCESSORS.**

YOU CAN HAVE YOUR CAKE AND EAT IT TOO

Processors need to consider how to optimize and maximize overall recurring revenue business over time, because that is where true long-term growth will come from. It's not an "either/or" decision of maintaining PCI non-compliance fees versus enabling merchants to be more compliant, sacrificing non-compliance fees in the process.

You can introduce a value-based service that helps customers get compliant and secure while at the same time also increasing non-compliance fees for those who don't switch and remain non-compliant.

Our market research regarding non-compliance fees shows that many processors are charging up to three times less than the highest non-compliance fees. However, to justify higher non-compliance fees you must offer viable alternatives for merchants such as the provision of security services facilitating merchant compliance.

Resulting in a neutral or positive outcome to the lifetime value of a merchant portfolio. Done this way the processor eliminates, or drastically reduces, liability (for example, in the event of class action suits for unexpected fees) and has an audit trail to justify any fee increases.

HOW DO YOU REPLACE **NON-COMPLIANCE FEE REVENUE COST-EFFECTIVELY?**

Income from the provision of managed compliance and security services provides the perfect alternative to non-compliance fee revenue. It turns a high-effort, negative-to-neutral PCI experience into a low-effort, positive experience for merchants.

HOW IT WORKS

1. An experienced agent relays the benefits of the program to the merchant, explaining that they will no longer have to pay noncompliance fees.
2. The agent offers to explain to the merchant why being PCI compliant is important and the benefits of putting security tools in place to protect their data.
3. The service begins when the agent forwards a link for the merchant to install the security application and tools on their devices.
4. While the app is downloading the agent guides the merchant through the compliance process from start to finish, validates their compliance with the PCI standard, and issues their certificate of compliance.
5. Once the app and tools have downloaded and installed, the merchant can avail of a range of security scans and tools including advanced endpoint security. The mobile app integrates into the suite of tools, exponentially increasing the merchant's ability to respond in real time and take action against possible threats.
6. The Services Operation Centre (SOC) will remotely monitor the merchant's security and will reach out if major incidents are detected.
7. The merchant receives reminders to run scans and perform any necessary tasks throughout the year and contacted again when it is time to renew their compliance.

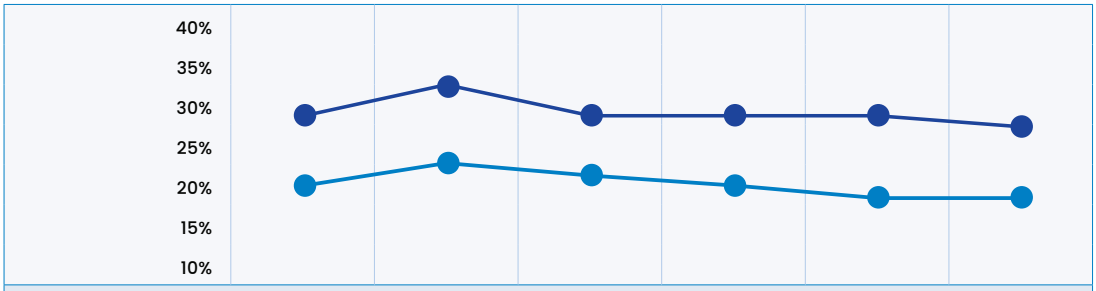
Key to the above is delivering appropriate, enterprise-grade security tools to these smaller merchants at an affordable price which is only possible when done at scale. Partnering with world-class security vendors for delivery to millions of businesses means security tools can be included in the managed service and delivered to merchants at an affordable price. Relevant security tools for small and medium-sized businesses include — ***Scanning Tools (ASV, Web, Cardholder Data, Device Security, Network Discovery), Antivirus, Endpoint Protection, Keyboard Encryption, VPN for mobile, Data Backup, Password Manager, Data Breach Protection, plus educational support around issues like Secure Remote Access.***

THE PRIZE FOR HIGH GROWTH **ANNUAL RECURRING REVENUE IS BIG**

Reducing attrition is fundamental to recurring revenue, and the market highly rewards growth for recurring revenue businesses. Merchants who subscribe to a Managed Compliance and Security service are less likely to move to another provider. When they value the service and the security tools, they are far more engaged and loyal.

An analysis of both self-service and managed service programs across six clients shows that managed program attrition performs 31% better[2] than self-service attrition. The chart below shows how merchants in a managed program, month-on-month, attrit at a lower rate than those in a self-service program.

CUSTOMER AVERAGE (GROSS ATTRITION RATE)



	A	M	J	J	A	S
Managed Service	20%	22%	21%	20%	19%	19%
Self-service	29%	32%	29%	29%	29%	28%
Δ % | Ms - Vs - SS	(32%)	(31%)	(30%)	(33%)	(32%)	(31%)

Gross Attrition Rate Managed Service vs Self-Service

[2]Analysis of merchants using VikingCloud's self-service and managed services programmes.

WHY **RETENTION MATTERS**

It typically costs five times as much to acquire new revenue than it does to retain existing revenue

89% of companies see customer experience as a key factor in driving retention

The probability of acquiring a new customer is only 5% to 15% likelihood whereas selling an existing customer a new product is 60% to 70%

Processors can credibly increase non-compliance fees up to threefold if they introduce services to enable merchant compliance

The average life cycle of a merchant is typically 3-5 years for processors so the loss of a new customer represents potentially 3-5X the ARR plus any lost upsell opportunities in addition to the current in-year revenue

Recurring revenue is critical to the health and growth of all payment processors so when a merchant cancels their account, you must consider the multiple year(s) of lost revenue that you now have to replace by signing up a new merchant. Plus, you don't only lose the recurring revenue, you also lose potential revenue from the upsell of additional products and services.

While high margin non- compliance fees seem appealing, they are short term gains at the expense of long-term recurring business. Additionally, it will cost five times the investment to make up for the lost revenue as opposed to a relatively small cost to keep it.

CONCLUSION

Maintaining the status quo by continuing with current, punitive non-compliance fees is a short-term play. The result is often increased attrition as merchants simply move to another provider who claims they can 'make the fee go away'.

Playing the long game, by replacing non-compliance fees with the provision of managed compliance and security services, reduces churn and increases customer lifetime value. This also results in an improved overall compliance and security status of the processor's merchant base. It is a win-win situation for merchants and processors. Merchants receive valuable services that save them time and money.

Processors increase their revenue, avoid the costs associated with customer churn, avoid negative regulatory attention, and reduce the sales effort needed to simply maintain market share - enabling them to focus on real growth in both volume and value.

IT IS A **WIN-WIN SITUATION FOR MERCHANTS AND PROCESSORS**. MERCHANTS RECEIVE VALUABLE SERVICES THAT **SAVE THEM TIME AND MONEY**.

VIKINGCLOUD™

REQUIRE **CYBER SECURITY AND COMPLIANCE** SOLUTIONS?

If you would like to find out more about our Cyber Security and Compliance Solutions; then please send an email to **sales@vikingcloud.com** and a member of staff will contact you.

About VikingCloud

VikingCloud provides end-to-end security and compliance solutions to businesses around the world, offering the latest in cloud-based solutions to secure networks and maintain compliance.

Almost 5 million businesses use VikingCloud's award-winning platform, and the company maintains partnerships with many of the world's leading acquirers and payment service providers. VikingCloud also works with the world's largest brands helping them proactively mitigate evolving cyber threats and business risk.

VikingCloud's Asgard Platform™ processes billions of security events daily, providing real-time intelligence access to an organization's cyber risk landscape.

Headquartered in Dublin, Ireland, with operations in the United States, Australia, Brazil, Canada, Germany, India, Mexico, Philippines, Poland, South Africa, and the United Kingdom, VikingCloud has clients in more than 70 countries and a global team of more than 1,000.

VIKINGCLOUD.COM