



# Why you need to rethink your PCI DSS strategy.

If you think your contact center is safe, you're wrong!

CARD-NOT-  
PRESENT CRIME  
IS SET TO REACH  
**\$7.2** BILLION  
BY 2020.\*

Even if your contact center is PCI DSS compliant, you are still at serious risk of a breach. This guide will help you understand some of the challenges businesses face, where you may be exposed and why you need to rethink your PCI DSS strategy.

See the 9 reasons why. 



## 1. Compliance doesn't equal security.

There's a false sense of security that if you're PCI DSS compliant, your contact center isn't at risk. Using multiple solutions can still lead to fraud. For example, pause and resume still allows your agents to see and hear card information, and isn't always reliable. And clean rooms require calls to be transferred, resulting in a poor customer experience. Both are technically compliant, but are not completely secure.



## 2. PCI DSS is a moving target.

There's no guarantee that today's solutions will work in the future. Compliance regulations will just keep changing and security auditors will find new gaps and vulnerabilities, which means you'll have to keep changing too. Also, even if you are compliant, you may still be at risk of a breach.



## 3. You're wasting time and money trying to keep up with PCI DSS regulations.

You need to protect your company's brand value, keep your customers' personal data safe and secure card data in your contact center. That's a tall order. But with every regulation change, you have to constantly change processes, implement new technology, maintain those solutions and spend time training agents. The operational costs can get out of control.



## 4. Contact center crime is a growing issue.

As online and point-of-sale transactions get more secure, criminals are now targeting the contact center. According to a 2018 study, card-not-present fraud is now 81 percent more likely than point-of-sale fraud.\* If credit card data is entering the contact center environment at all, where agents can see or hear it, or if it's being stored in your systems, it's at risk of being stolen.

\*2018 Identity Fraud Study, Javelin Strategy & Research

<https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin>



## 5. Pause and resume and other BAND-AID® type fixes are not the answer.

Manual interventions are simply not reliable enough. Agents can still see and hear card details. Interrupting the call by transferring to an IVR or clean room environment is a less than ideal customer experience and these solutions have less than stellar success rates.

The average U.S. company uses **3** different solutions to maintain PCI DSS compliance, which is costly and time consuming.



## **6. Your PCI DSS solution is inhibiting your contact center technology progress.**

Once your contact center environment – IVR, switch, payment service provider, network – are embedded into your compliance process, it becomes problematic to change them when new regulations are introduced. You have to redo the plumbing and wiring again at great expense in terms of time and money.





## 7. The cost of cyber insurance is climbing.

In order to get lower premiums, you need to protect customer data to the greatest degree possible. Many solutions leave you more exposed to increased premiums. A 2017 Ponemon Institute survey found that 87 percent of companies view cyber liability as one of their top ten business risks. The average cost of a cyber breach was \$349,000 for small companies and \$5.9 million for larger organizations.



## 8. PCI DSS challenges prohibit you from benefiting from Work at Home Agent environments.

There are many advantages to having remote agents, but a multi-solution approach to PCI DSS compliance creates security and training challenges that are difficult to overcome, leaving fewer choices and less flexibility in staffing your contact centers.



## 9. Poor customer payment practices can lead to lower CSAT/NPS scores.

Customers expect their financial information will be kept safe and secure. Requiring customers to read data aloud over the phone is a risk and can lead to higher levels of dissatisfaction. Customers want to pay in their channel of choice. Shifting them to another channel such as a payment IVR or clean room environment can be very frustrating.

There is a better way:

## CallGuard from Eckoh.

Significantly reduce your risk of fraud and streamline your compliance process with one simple solution.

Eckoh's patented CallGuard uses DTMF masking to prevent credit card data from ever entering the contact center environment, which means all of your contact center can be removed from PCI DSS audit scope. Agents can't see or hear it, but remain in constant contact with your customers, providing a great customer experience. CallGuard fits around your existing systems allowing you the flexibility to change what you want to change, when you want to change it.

# The CallGuard experience.



## Card Data Input

When the customer is ready to make a payment over the phone, the agent simply asks them to enter their payment card data on their phone keypad.

## Agent Experience

The agent NEVER hears the DTMF tones, or sees a card number or CVV. In addition, no card data will be captured on screen, in call recordings or enter any part of your network.

## Customer Experience

The customer and agent are in constant contact throughout the call, making for a great customer experience and reduced handling time.

### **Future Proof**

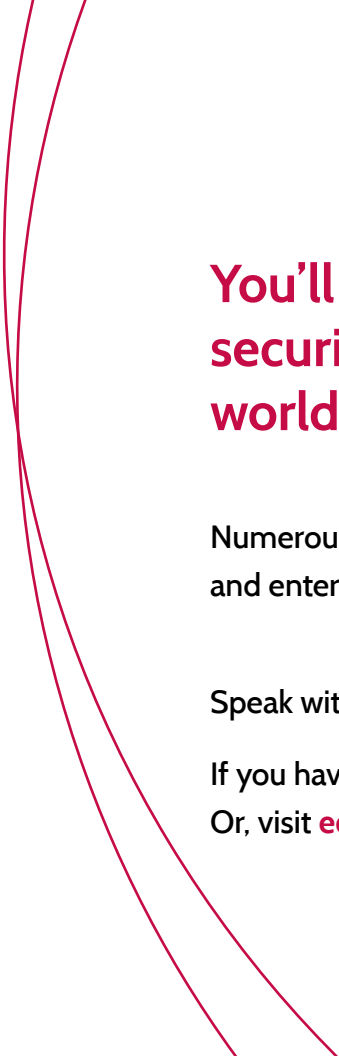
CallGuard doesn't tie your hands to any existing systems or payment processes. You're free to make changes at any time.

### **Light Touch**

Eckoh does all of the heavy lifting, greatly reducing the burden on your IT staff. There are no APIs to write to and no integration necessary with existing systems.

### **Secure**

Not only are you compliant, more importantly, you're secure because the card data never enters your environment.



**You'll have the flexibility you demand, the security you need and be backed by the world's leading provider of secure payments.**

Numerous Fortune 500 businesses in the retail, insurance, travel, leisure, and entertainment sectors choose Eckoh to secure their payment data.

Speak with one of our security experts at **866-258-9297**.

If you have questions, email us at **[tellmemoreUS@eckoh.com](mailto:tellmemoreUS@eckoh.com)**.

Or, visit **[eckoh.com/us/security](https://eckoh.com/us/security)** to learn more.

The logo features the word "Eckoh" in a bold, sans-serif font, centered within a white circle. A small grey dot is positioned above the letter 'h'. The entire logo is set against a dark grey background.

**Eckoh**

Eckoh<sup>•</sup>