CardEasy™
Securing Contact Center Payments

CardEasy market research report 2023

Consumer attitudes to card payment security:

Are organizations doing enough to secure payment card details?

Background to the research

We have been conducting this research regularly since 2014, giving us a long-term perspective on changing consumer attitudes. We last conducted it in 2021. Much has changed since then. In 2021 we were in the thick of the COVID-19 pandemic and businesses were scrambling to adapt to the new reality of remote working and a huge growth in online shopping. Now the world has returned to something approaching normality, this is a good time to review the state of the payments industry and see to what extent the pandemic has changed to consumers' attitudes and whether the changes we saw during the pandemic are likely to be permanent.

Methodology

This research updates our 2021 publication The future of secure omni-channel payments in a post-pandemic world by reviewing the current state of play regarding consumers' attitudes to payment by phone.

There are three key elements to this research:-

- A review of current published research on the topic
- Telephone interviews with a variety of experts from across the industry
- A survey of 456 consumers in the UK and US

How the payment landscape has changed since 2021

Payment card fraud has boomed during the pandemic

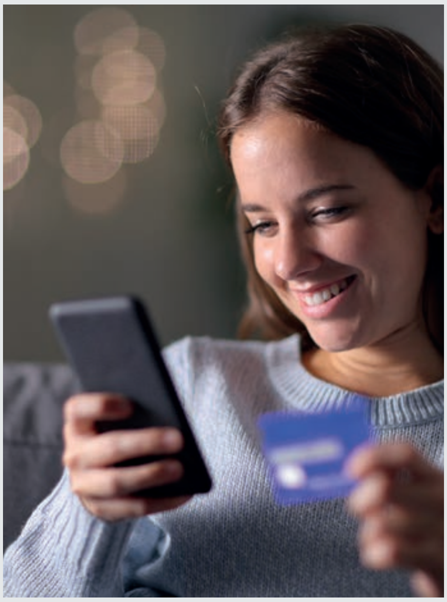
The telephone remains an important channel, and the pandemic has reinforced that rather than diminished it. The number of card payments increased substantially during the pandemic largely because both retailers and consumers switched to using cards rather than cash due to a (now known to be incorrect) perception that the virus could be transmitted much more readily via the handling of cash than by contactless card payment. In the UK, for example, card payments were 75% higher in April 2020 than they had been in the previous year. At the same time the limit on contactless payments increased to £100, making them an even more attractive option for consumers. This then led to a boom in payment card fraud.

408 million

data records breached in 2022

"For the last ten years or so we've been hearing that call volumes are going to decrease whilst digital volumes are going to increase...But in fact, we haven't seen huge a decrease in call volumes so voice is still hugely important to organizations, in part because of the pandemic."

Juergen Tolksdorf is Senior Director of Marketplace Innovation at Genesys

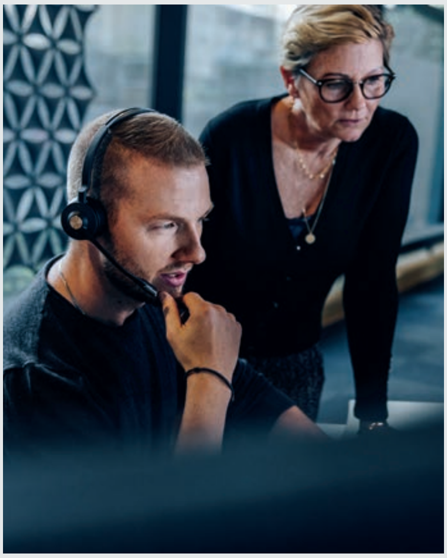


As many more consumers moved to online shopping and digital banking, so the fraudsters followed them. Truist in the US (formed out of a merge between BB&T and SunTrust) reported fraud claims growing from 37,000 annually to 26,000 per month. The financial website Fool.com reports that 2021 was one of the most eventful years on record for identity theft and payment card fraud. IT Governance reports that 408 million data records were breached in 2022 - a slight fall from the all time high levels of 2021 but still a significant number indicating organizations need to remain vigilant.

These alarming figures show that consumers are right to be concerned about payment card fraud. The pandemic has had an extremely negative effect on consumers' perceptions of payment card safety, as a rational response to increased risks that consumers faced during that period.

> **"Our customers want to know that their card details are safe. We don't store their card details in any way. It's all about giving our customers that peace of mind. As a contact center agent, if you call and make a booking with me, I don't have access to your card details. You don't have to worry about your card details being fraudulently used by somebody because they are never exposed. The benefit for us is the customer's peace of mind."**
>
> **Marc Bainbridge, Head of Integrated Services at Hurtigruten**

There is some good news. Whilst payment card fraud has increased, the overall number of data breaches has declined. Fewer overall data breaches were reported in the US in 2022 than in 2021. The Identity Theft Center's Business Impact Report 2022 suggests that there may be two factors particularly relevant here. One is the effect of the ongoing war in Ukraine which has reduced the activity of cybercrime groups based in Russia, and the other is the fact that small businesses have increased investment in security tools and staff training, meaning they are less vulnerable to data theft.



That said, the report also acknowledges that phishing and social engineering attacks aimed at employees or contractors with access to sensitive customer data are growing ever more sophisticated and harder to stop. There is also a continued risk from intentional fraud committed by or with help from call center agents themselves. Research from Fraud.com shows that five percent of call center agents have been intentional participants in some form of insider fraud.

65%

of organizations reported that they had seen an increase in cyberattacks in 2022 that they attributed to greater levels of remote working.

The increase in remote working presents more opportunities for payment card fraud

Data breaches and other compromises due to the use of remote workers rose from 25% of all breaches in 2021 to 35% in 2022 due to the growing trend for working from home. Organizations are now supporting on average twice as many remote workers than they were before the pandemic.

> "I believe the pandemic has forced businesses to be more resilient and to make sure there are more contingency plans for future proofing. For example, we now have the capability for staff to work from home or in the office. I also think most businesses will also be more cautious as a result of the pandemic. "

Graeme Simpson, UK Application Support Analyst, Hiscox UK

Whilst numbers of remote workers have fallen back somewhat since the peak of the pandemic, many organizations have switched permanently to this model of working. In 2022 organizations reported 41% of their workers would remain remote, necessitating a significant adjustment of security protocols and throwing up a number of security challenges as 78% of organizations say that remote workers are harder to secure. 65% of organizations reported that they had seen an increase in cyberattacks in 2022 that they attributed to greater levels of remote working.

The only way to ensure card data is secure is to prevent it from entering the contact center network environment in the first place

Thus, it remains the case that the most effective way of ensuring the security of payment card data in a contact center is to make sure that data does not enter the network environment in the first place and that neither employees nor contractors are ever exposed to it. As soon as sensitive card data is allowed into the contact centre environment then the organization is at risk of theft and fraud.

Another significant change since our last research report is the introduction of PCI v4.0 in 2022. This latest version of the PCI Standard recognises that the threat landscape has changed and that ongoing security is vital to protect payment data. It aims to encourage organizations to see security as an ongoing and continuous process and to promote flexibility, giving organizations a range of different methods that they can deploy to achieve their security goals.

The advice of the PCI Security Standards Council has always been that organizations should not store cardholder data unless it is absolutely necessary.

> "Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves...In general no payment card data should ever be stored by the merchant unless it's necessary to meet the needs of the business."

PCI DSS Security Standards Council

Only 8%

of US consumers believe organizations they buy from over the phone will keep their card details secure

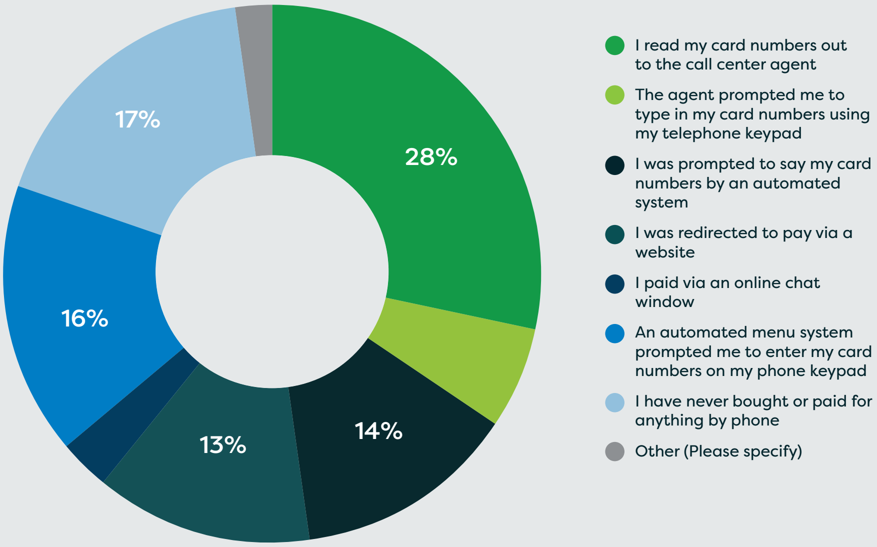
Changes in consumer attitudes since 2021

In 2021 17% of consumers strongly agreed that organizations they bought from over the phone would keep their personal and card details secure. In 2023 this percentage remains the same amongst UK consumers but in the US it has dropped down to 8%, **meaning that US consumers are significantly more concerned about payment card security and less trusting of organizations now than they were before the pandemic.**

In our 2018 research report 76% of consumers agreed with the statement that 'despite careful recruitment policies some contact center agents may commit card fraud directly or indirectly by stealing personal data and credit card payment details they take from consumers over the phone.' In 2021 this fell to 59% but in 2023 this number is back up to 76%, again suggesting that consumer attitudes have hardened since the pandemic.

In 2018 49% of consumers said that the last time they bought something by phone they had been asked to read out their card details to the agent. In 2021 this percentage fell significantly to 23%. In the UK it has continued to decline – only 18% of UK consumers report being asked to pay this way in 2023 however in the US the percentage is rising with 28% now saying that they were asked to read out their card details the last time they bought something.

The last time you paid for something over the phone, how was payment taken?



Consumers are very reluctant to give out their details by phone

70%

of US consumers are reluctant to make payments by telephone because they fear their card details will not be kept secure

62% of US consumers (and 70% of UK consumers) now agree or strongly agree that the risk of contact center fraud stops them from making payments over the phone.

> **"I prefer not to pay this way [reading card details to an agent] if it's not required. I'm very concerned when I have to make payments this way."**

> **"I would feel more comfortable [giving my card details] if I knew that the agent could not hear or see my card details"**

Similarly, 70% of US consumers (75% in the UK) state that they are reluctant to make payments by telephone. Thus, it is clear that companies who ignore this or fail to take customers' payment card security seriously will certainly be losing business as a consequence.

"Consumers don't want to give their credit card number to contact center agents. That's certainly something which is not going to fly anymore, so PCI compliant vendors need also to focus on providing the right technology to simplify the customer experience. This is where providers like CardEasy which enable seamless and secure payments across multiple channels have a big advantage."

Juergen Tolksdorf is Senior Director of Marketplace Innovation at Genesys

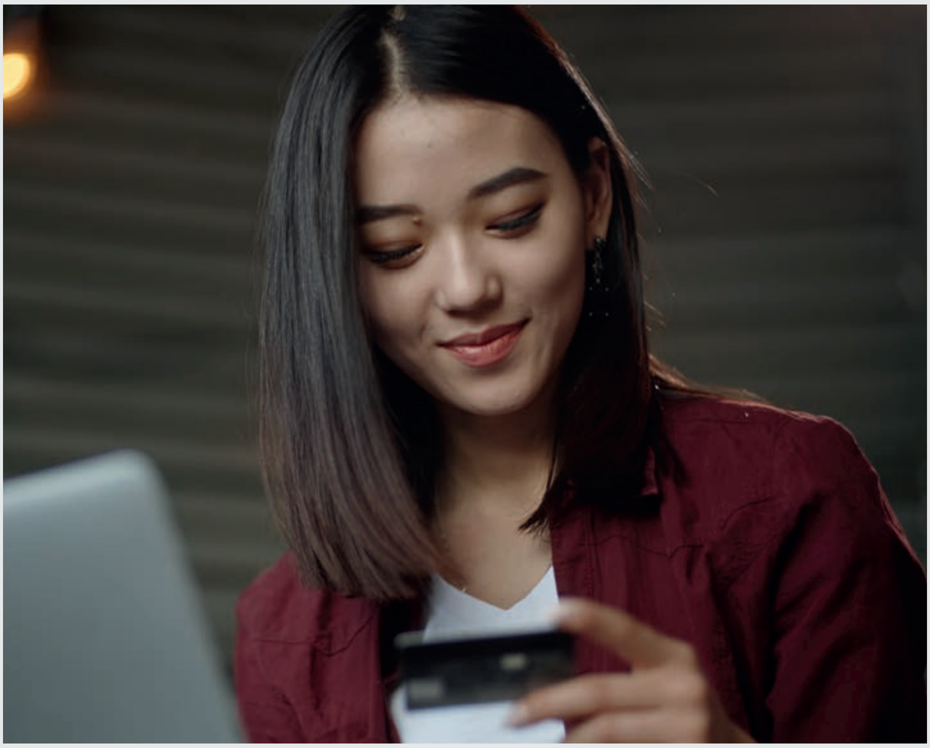
> **"[Payment card security] has become more of a concern to people in the last couple of years. When we did roll [CardEasy] out...the response was positive and [customers] said that they were happy to see that we were implementing a more secure method of collecting credit card information."**

Large US Online Retailer

One of the big benefits of implementing a secure payment system such as CardEasy is that it clearly demonstrates how seriously the company takes card security, reassuring customers who are concerned.

> **"The main benefit for us is that our customers know that their card details are safe. We don't store their card details in any way. It's all about giving our customers that peace of mind. As a contact center agent, if you call and make a booking with me, I don't have access to your card details. You don't have to worry about your card details being fraudulently used by somebody because they are never exposed. The benefit for us is the customer's peace of mind."**

Marc Bainbridge,
Head of Operations



Only 30%

of consumers agree that home-based workers are just as secure as those working in a contact center

Do consumers care where contact center agents are based?

The trend towards working from home during the pandemic affects both contact center agents and consumers. Half of survey respondents in the US (50%) and 62% of UK consumers agree that they have worked from home more since the pandemic than they did before, and their expectation is that this will continue for the foreseeable future.

Most consumers state that they do not care whether the contact center agent they're speaking to is based at home or in the office – just over 60% agree that this makes no difference. However, they do perceive a difference in security between home and contact center workers. Less than 30% agree that home-based contact center workers are just as secure as those working in contact center.

	Strongly Agree	Agree	Disagree	Strongly Disagree	Don't Know
It makes no difference to me whether the person I am talking to is working in a contact center or working from home.	21.59%	40.09%	19.38%	10.13%	8.81%
Home-based contact center workers are just as secure as those working in the contact center.	8.81%	21.76%	32.21%	20.21%	17.10%

> **"With all of the cyber threats and security issues that are going on today it's very important for us to provide enhanced security as far as customers are concerned. We take security very seriously here, as do our customers."**

Craig Schoeberle, Senior Director of IT and Infrastructure, Parts Town

Consequently, it is vital that organizations both take the security of remote contact center agents seriously and also are seen to take this seriously by their customers. Visible security measures provide the reassurance that customers need.

> **"We did have security concerns when our contact center agents started working remotely. This is where quality procedures and monitoring comes in. The fact that we had CardEasy already implemented made the process easier because it means that we are no longer asking our customers to provide their payment card details to our contact center agents."**

Marc Bainbridge, Head of Integrated Services at Hurtigruten

Customers expect a seamless omnichannel shopping experience

It's clear that consumers now expect to be able to take advantage of a seamless omnichannel shopping experience and that retailers who deliver this have a significant advantage over those who do not. As McKinsey argues "Offering a compelling omni channel experience used to be the bleeding edge of retail. Now it's a requirement for survival."

Our research backs this up. Over 80% of consumers agree that it's important to them to be able to contact a company via whatever method is most convenient to them, and over 60% agree that they like to be able to switch between channels when dealing with companies.

80%

of consumers agree it's important to be able to contact a company via whatever method is most convenient to them

	Strongly Agree	Agree	Disagree	Strongly Disagree	Don't Know
I prefer to deal with companies by phone or Internet than in person	21.59%	41.48%	20.09%	15.72%	5.68%
I think dealing with companies remotely has become the norm now	21.05%	59.21%	7.46%	6.14%	6.14%
Its important to me to be able to contact a company via whatever method is most convenient to me	37.12%	21.76%	46.29%	9.61%	1.31%
I like to be able to switch between channels (e.g. from phone to email or live chat) when dealing with companies	14.98%	48.90%	11.89%	10.57%	13.66%
I think the switch to remote working is likely to be permanent	17.26%	47.79%	13.721%	8.85%	12.39%

> **"I want you to remember me because whenever I come back and buy more stuff, I don't want to have to think about entering my credit card number, my CVV. I don't want to have to think about any of that."**

Alex Pezold is co-founder of TokenEx

This puts pressure on organizations – retailers in particular – to provide consumers with a truly omnichannel experience, whilst simultaneously ensuring that their payment details are kept secure across all channels. An effective and secure card payment system can facilitate this.

"Before, we found that the direct sales team were so busy that we were almost certainly losing customers who weren't prepared to wait in a call queue. Now that the customer can pay over the phone directly with the store, we have been able spread the load, so we're getting fewer calls into the contact centre which means improved call handling times. Customers are also able to talk to the local store that they've been dealing with which we think is a significant improvement to the customer journey.... I've been a customer myself of Sofology and I used the omnichannel options. I found it quite useful to go into the store, have a look at what I wanted, build the basket, go home, have a think about it. Personally, as a customer, I found it really good and I'm pretty sure the other customers do as well ... it's definitely adding a lot of value to the business."

Ashley Hill, IT Service Delivery Manager

Which telephone payment method do consumers prefer?

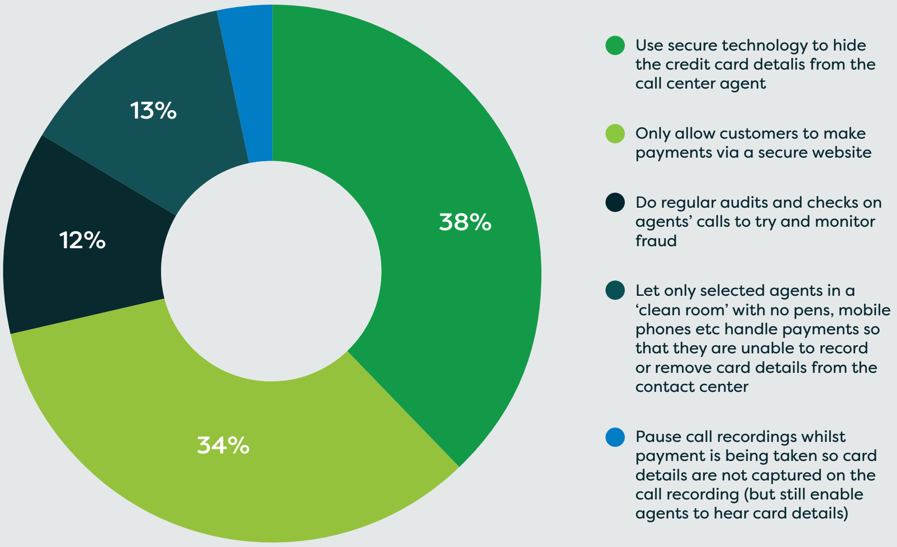
This research clearly shows that organizations still have some way to go when it comes to convincing consumers that their payment card details are secure. The increased threat of payment card fraud combined with the move towards working from home and consumers' growing expectations as regards a true omnichannel purchasing experience mean that offering visibly secure methods of card payment offers organizations a true competitive advantage.

Consumers show a clear preference for technologies that reliably hide payment card details from contact center agents - 70% believe that using such technology is secure, compared to only 33% for so-called 'pause and resume' solutions.

70%

of consumers believe that using technology that reliably hides payment card details from contact center agents is secure

How should organizations best avoid fraud in contact centers?



> **"This [entering card details via the telephone keypad] seems like a more secure method than dictating my card details to a person."**

> **"Paying with inserting your card info on your phone keypad will make things much better"**

> **"I feel much more secure when not having an agent on the line and just having to key in the payment information on my phone."**

About CardEasy

All CardEasy solutions are built around your contact center and practices, meaning your operations remain as you want them. We work with you to protect your customers' data, as well as your company's reputation.

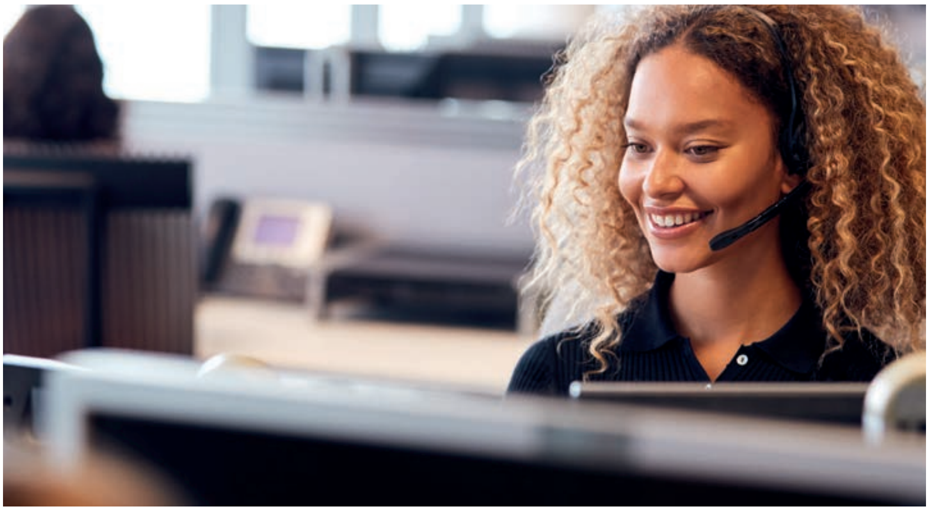
CardEasy removes the risk of payment card fraud within your contact center by preventing your contact center agents from hearing or seeing payment card data, using DTMF suppression to automatically block it from your screen and call recording (without the need for a pause/resume function) and preventing it from entering your contact center systems and networks.

Our patented technology creates a secure payment environment for payments handled over the phone, self-service IVR payments, as well as payments via email, webchat, SMS, social media or even via video calls.

Using CardEasy saves you time and money by taking your operations out of scope from PCI DSS controls, whilst removing the need for time-consuming oversight and PCI audits. Not only can it improve your call handing times and your customers' experience, but setup costs are low, and ongoing managed service costs can be linked directly to your channel or agent utilization.

CardEasy enables you to comply fully with PCI DSS as follows

- Your agents will not be exposed to customers' payment card data, wherever they are working from
- Payment card data will not be stored in your call recordings or captured in screen recordings
- As the payment card data will not enter your contact center environment or network, this de-scopes the whole environment from PCI DSS regulations and audit requirements
- CardEasy Agent Assist allows your agents to remain connected to your customers throughout the payment process, to provide guidance as required
- CardEasy also supports IVR payments for when no agent assistance is required, such as balances payable, utility bills, charity donations and subscriptions
- CardEasy Digital enables your contact center to take secure payments via any digital channel such as email, webchat, SMS and social media
- CardEasy helps with GDPR compliance by avoiding the capture and storage of payment card data



All the CardEasy secure payment solutions work seamlessly together, as well as integrating with your existing systems, ensuring that your customers receive a consistent and user-friendly payment experience whatever channel they decide to use.

Whether you choose to use CardEasy for agent assisted, IVR or digital payments (or all three), your customers' payment card data is never seen or heard by your agents, or stored in your environment or call recordings, meaning your environment is fully de-scoped from the PCI DSS controls.

What our customers and partners say about CardEasy

sofology

"The level of engagement we've had from the CardEasy team has been great. The selling points of CardEasy are that it has an attractive price point and its ease of use, but the biggest selling point, certainly from my perspective as the IT service delivery manager, is the level of service that we get from the CardEasy team. For me, that's worth its weight in gold."

Ashley Hill
IT Service Delivery Manager

worldpay

"Worldpay is a recognized leader in security and risk management. Our joint proposition with CardEasy offers a secure transaction service while removing the need for contact centers to have onerous annual PCI audits."

Keith Dallas
Chief Product and Marketing Officer

realex payments

"Realex is delighted to be partnering with CardEasy, which is fully integrated with the Realex payment gateway. This enables our merchants to de-scope their contact centers, outsourcers and home-workers from PCI DSS regulations and audits, whilst providing seamless and secure MOTO transactions."

Head of Partnerships

HISCOX

"Overall we're very happy with CardEasy. We need systems that support our high-quality customer service ethos and meet our commercial requirements and, in our case, CardEasy matches those needs and does exactly what it promised."

Sean Carney
Head of Operations

AIB

"The CardEasy solution easily de-scopes us from PCI DSS compliance and mitigates the risk of any internal fraud. The platform is scalable and easy to use...along with the confidence we have in the CardEasy team who have been instrumental in a smooth implementation, guiding us and offering insight."

Eoin Heneghan
Head of Collections

Micron

"We have been impressed by the flexibility, ease of integration and support of the CardEasy system, as well as its PCI DSS security to protect in-house operations and our outsourced service providers in the USA and EMEA."

Gary Lazarowics
Head of eCommerce & Sales Support

Staples

"CardEasy was the perfect fit to resolve the PCI compliance and data security needs in Staples' major contact centers in Europe. This was because of its ease-of-use, the breadth of PCI DSS issues it resolves in one go, the flexibility of integration with all our differing systems and the ability for them to meet our tokenization requirements."

Albert de Vlieger
Senior Strategic Alliances Manager

ingenico GROUP

"Ingenico ePayments is integrated with CardEasy to keep card data out of the contact center environment altogether, thus taking you out of scope of PCI DSS controls without compromising customer experience."

Eoin Heneghan
Head of Collections

First Data

"Solutions such as CardEasy are the new industry standard for PCI DSS compliant MOTO payments by phone. Our integration and strategic partnership with CardEasy let merchants satisfy all the key PCI controls within their contact center environment with just one solution. It is also better trusted by customers than having to read their card numbers out, whilst also improving the customer/agent experience and reducing call handling times."

Richard Simon
Commercial Director

What our customers and partners say about CardEasy

LOCUS TELECOMMUNICATIONS, LLC

"We chose CardEasy because it was the solution that we needed to de-scope our contact center agents and IVR environment. CardEasy was the only vendor that provided the flexibility to integrate with our home-grown systems because their system can be cloud-based, with no requirement to change any of our existing IT."

Carlos Moreno
Payment and Fraud Analyst

HURTIGRUTEN

"The professionalism with which the CardEasy team approached everything was second to none. They fully supported us and bent over backwards to ensure we were PCI compliant. They are always quick in their approach and have assisted us in areas where they did not even have to, which is a testament to their professionalism. CardEasy is simple and easy to use and takes away the risk as our customers know their card details are handled securely."

Marc Bainbridge
Head of Operations Support

Miele

"Miele selected the hosted CardEasy system to enrich customer service whilst de-scoping us from large sections of PCI DSS regulations, which otherwise require significant cost and effort to satisfy."

Paul Aram
IT Manager

AVON

"One of the good things about CardEasy is that it is payment processor and acquirer agnostic so you have one solution that fits all of your needs. Generally, the amount of effort that the CardEasy team has had to put it in from an integration perspective has been very little, which has been really good. Confidence levels are high. Everything is good."

Jason Earnshaw
SSC Technology and Projects Manager

Partstown

"The folks at CardEasy are amazing to work with. They're very responsive, very professional, very technical. They really know the product and they're very passionate about it. They align with our core values at Parts Town. We're big on innovation, passion, courage and integrity – all that good stuff – and the CardEasy team are as well. It's been a great experience. We love working with the CardEasy team."

Craig Schoeberle,
Senior Director IT and
Infrastructure Management

CardEasy™
Securing Contact Center Payments

Contact us to arrange a demo or find out more

We'd love to hear from you. If you have any questions about CardEasy or would like to arrange a demo or talk about how it might work for your organization, please don't hesitate to contact our sales team.

☎ **UK: +44 (0) 20 7741 2000**

✉ **sales@cardeasy.com**

☎ **US: +1 303 500 0492**

www.cardeasy.com

PCI Security Standards Council®

CardEasy is a trading style of Syntec Limited. Registered in England and Wales No: 03529985 | Version 1.0 Apr23