pcipal®

SECURITY IN THE CONTACT CENTER

A Comparative Study of Consumers
and Contact Center Professionals

CONTENTS

GET IN TOUCH

U.K. ☎ +44 207 030 3770

U.S. ☎ +1 866 645 2903

✉ info@pcipal.com

www.pcipal.com

FOREWORD

In July of this year, PCI Pal conducted a survey with consumers and contact center professionals in the U.S. and U.K. The consumer survey was concerned with sentiments about their digital preferences, security perceptions, and beliefs about future trends in the customer service space. Do you believe you will interact more with contact centers over the next five years? Will new security exploits endanger customer privacy? Will it become ever more difficult for callers to speak with an agent instead of a digital assistant? Contact center professionals - including agents, management, and senior leadership – were asked for their thoughts on how the industry has changed over the past year and what that means for the future, and how confident they are with their organizations' ability to handle customer inquiries.

The coronavirus and its effect on the workplace and on consumer behavior have, of course, changed our lives, our consumer habits, our workplaces, and consumer and contact center surveys alike reflect that shared experience. That said, there's more to the story of contact centers in the 2020s than COVID, and the research findings highlight additional areas of focus for this vertical.

Even before 'coronavirus' entered our lexicon and upended our daily lives, the tech and security worlds were undergoing change. Artificial Intelligence (AI) and machine learning are making a big impact the world over, and now billions of devices comprise an entire Internet of Things. High-speed broadband and 5G are expanding their reach daily, even as rockets continue to launch satellite internet. The world has transformed in innumerable ways in the forty years since I began programming on a Commodore 64, and in the 2020s the rate of change has, if anything, accelerated.

All these new technologies are fascinating in and of themselves, but it doesn't take long before hackers start to find the security flaws and exploit them. Cybersecurity professionals, as well as everyday consumers, must remain vigilant in the face of these innovations.

New technologies and new ways to transact introduce new potential problems. In these pages, you'll hear about contact center challenges, customer concerns about how their data is handled in the age of machine learning, and wariness about social media purchasing. You'll also gain a fresh perspective on what contact center professionals — from frontline agents to senior management — have observed over a tumultuous 18 months. We'll share the different predictions for the future of digital security that contact agents, management, and customers make.

While there are striking differences between management, agent, and consumer thinking, as well as gaps between British and American perspectives of digital security, there are constants that all professionals should focus on. One finding that comes across again and again throughout the research: Cybersecurity is a global team game. Everyone, from consumers to contact center agents to IT teams to management, has a role to play in accomplishing the greater good: a safer and more secure environment for everyone.

Geoff Forsyth

CISO, PCI Pal

INTRODUCTION

Since March 2020, almost every industry around the world has experienced sustained shocks and continuous upheaval. Businesses that were designed to operate face-to-face went remote almost overnight; many firms that required in-person interaction failed and were shuttered permanently. By necessity, everyone adapted to new ways of conducting their daily lives.

The pandemic accelerated social and technological trends, including those related to security and privacy. In February 2020, few people beyond epidemiologists recognized the term 'contact tracing', but by April and May, governments across the world were practicing it. People who'd never placed an online order in their lives began subsisting on grocery delivery apps, and much retail shopping went entirely online. A world that prohibits face-to-face interaction is, almost by definition, a world that demands multichannel or even omnichannel payment options.

All over the world, contact centers 'decentered' as agents moved to ad-hoc remote workplaces. At the first peak of the pandemic, many organizations received huge influxes of calls. The callers who attempted to reach financial institutions and government offices encountered busy signals or hours-long waits. The contact center agents and managers, for their part, had to learn new remote systems and ways of operating while a massive social, economic, and public health crisis continued.

In 2022 and beyond, what does the future hold for the contact center industry? The results of our new consumer research, conducted in Summer 2021 by AYTM Market Research (United States) and Atomik Research (United Kingdom) on behalf of PCI Pal, give some clues to the challenges and opportunities that the industry faces in the months and years ahead.

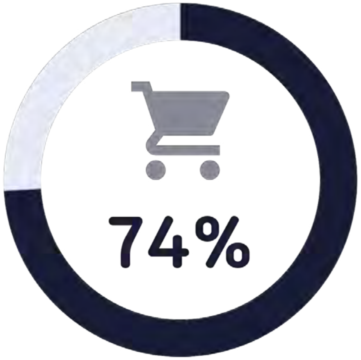
As we'll see, consumers and contact center professionals may not always agree on the central issues of the era, but their combined voices suggest paths forward.

SETTING THE SCENE

The surging Delta variant and the persistence of COVID-19 provide more than enough for an exhausted world to worry about, but hackers and scammers have not let up in the past nineteen months. If anything, they've redoubled their efforts. The United States Federal Trade Commission has even had to launch a page devoted to countering COVID scams. Similarly, local governments in the UK - from Cambridgeshire County Council to Bristol - have had to set up similar pages warning people of phishing and other scams relevant to COVID-19.

Meanwhile, hackers have no scruples about kicking hard-hit industries when they're down: Expedia, Booking,com, and Hotels.com have all suffered coronavirus-era attacks. Organizations that fail to protect consumers' information receive bad press and may be liable to paying fines. Such laws as Canada's Protection and Electronic Documents Act (PIPEDA), the European Union's General Data Protection Regulation (GDPR), and the Australian Privacy Act all prescribe strict punishments for negligent companies. American laws vary from state to state, but California's recent California Consumer Privacy Act may serve as a model for legislation across the country.

The fines these laws impose, however, are not the end of the damage: 74% of consumers are reluctant to shop with compromised firms for a few months after the bad news breaks. In times like these, very few businesses can afford to take that kind of hit - yet most businesses will have to have some interaction with credit card or bank account data.



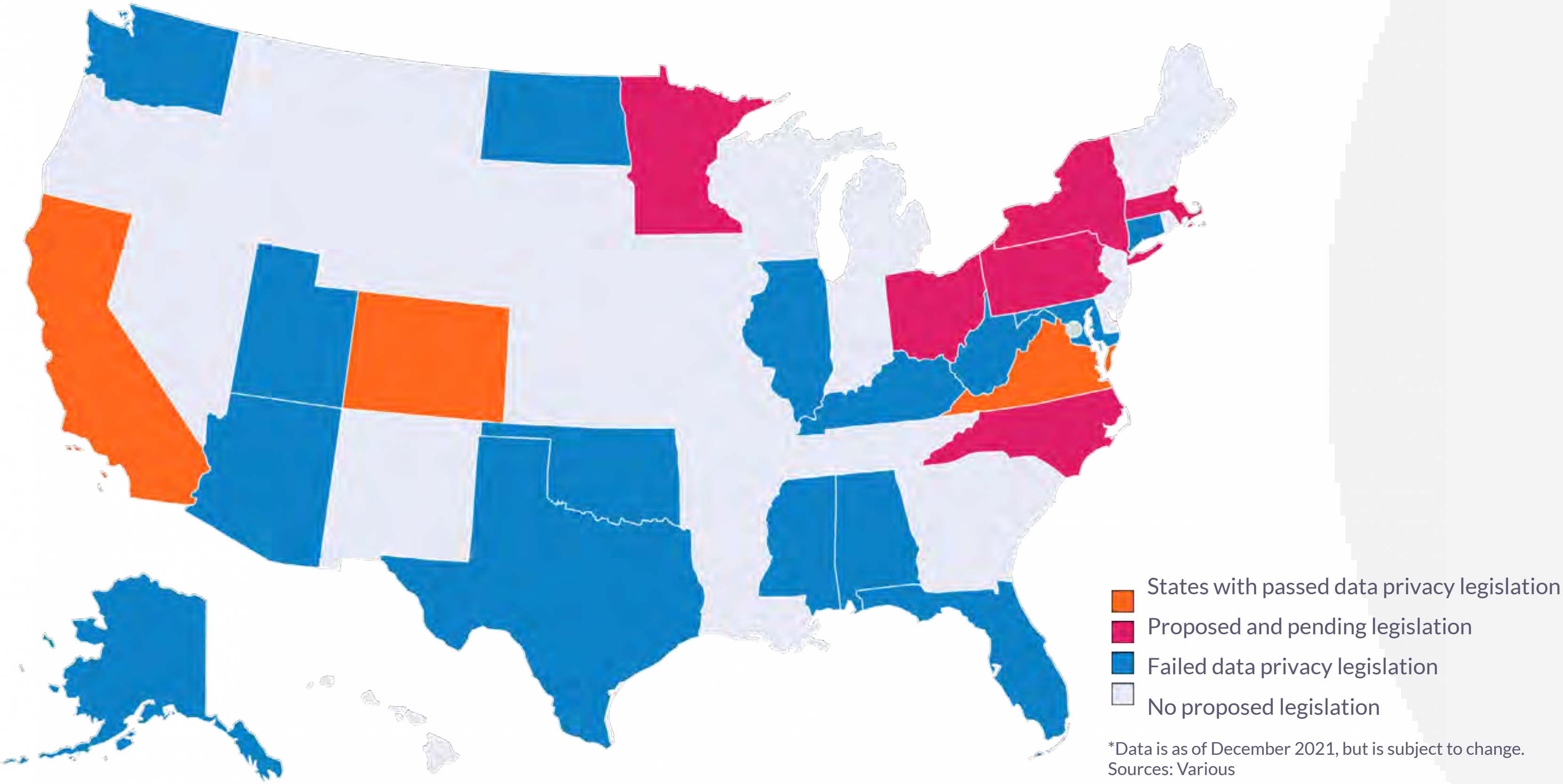
of consumers are reluctant to shop with compromised firms for a few months after a breach

New Frontiers for American Regulation

British businesses similar to those in Canada and Australia already operate under rigorous but fair data protection. In the United States, however, businesses in some jurisdictions may have greater responsibilities than their peers a state or two over. That may be set to change.

To date, four American states have passed comprehensive data security laws. California's Consumer Privacy Act is the best-known, but similar laws are also on the books in Maine, Nevada, and Virginia. Across the nation, red, blue, and purple states are all considering more robust privacy laws. These states include Alabama, Alaska, Arizona, Colorado, Connecticut, Florida, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, New Jersey, New York, Oklahoma, Texas, Washington, and West Virginia.

And while privacy and data regulation laws do vary from state to state, many organizations must adhere to federal laws like HIPAA, the Health Insurance Portability and Accountability Act. One way or another, almost every American organization has certain legally mandated data handling responsibilities, and as our lives grow ever more connected to the digital worlds, these duties will only increase.


🟧 States with passed data privacy legislation
🟥 Proposed and pending legislation
🟦 Failed data privacy legislation
□ No proposed legislation

*Data is as of December 2021, but is subject to change.
Sources: Various

Strategies for Tomorrow

Since transacting solely in cash is neither possible nor desirable for most businesses, how should they react to the rash of hacks, scams, and attacks?

The Payment Security Industry Data Security Standards, commonly called PCI DSS, appear intimidating: The document laying out the May 2018 revision runs 139 densely packed pages, and is full of acronyms, bulleted lists, charts, and tables. The basic principles of PCI DSS, however, are simple, and can be summarized in twelve principles.

Companies must:

- Complete an annual risk assessment
- Ensure third parties that store, process and/or transmit card data have maintained their PCI DSS compliance and are still registered with the card schemes
- If they use an integrator to bring the products together, make sure they are certified to the required standard to do so
- Train their staff to follow PCI DSS procedures
- Make sure they only store data that is essential and that it is encrypted and/or masked
- Protect their data network and make sure they are using a firewall and up-to-date anti-virus software
- Perform network scans on a quarterly basis. These must be performed by an Approved Scanning Vendor (ASV)
- Discuss security with their web hosting provider to ensure they have secured their systems appropriately. Web and database servers should also be hardened to disable default settings and unnecessary services
- Run annual pin entry device (PED) tests to identify any vulnerability, if using pin entry devices
- Only use software or hardware that has approval from the Payment Card Industry Security Standards Council (PCI SSC) to process transactions

Every item on the PCI DSS list makes intuitive sense, but properly instituting and maintaining them can constitute major hurdles for many businesses. Encryption, testing, training, and updates all take significant time and energy. The good news is that businesses have another option: They can 'descope' their operations so that they no longer have direct contact with customer data.

Let's explain. 'Descoping' might sound negative: Is a company that 'descopes' limiting the range and scope of its offerings? Quite the opposite.

Descoping frees up organizational resources to do more and better things by ensuring that businesses never directly interface with payment card data.

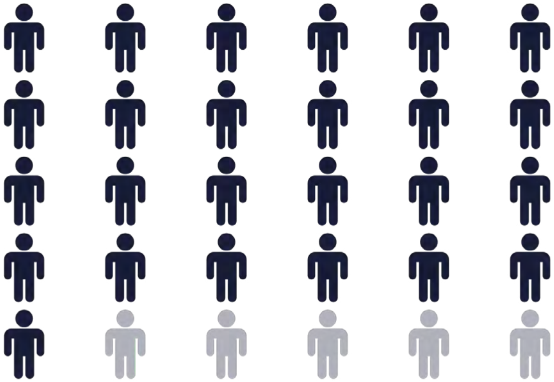
By collaborating with a service provider like PCI Pal, they keep sensitive data off their servers and out of their hair.

THE CONSUMER PERSPECTIVE

While chatbots and similar artificial intelligence solutions may appeal to contact center managers due to their flexibility, scalability, and affordability, public confidence in these tools leaves something to be desired. A staggering 81% of British consumers worry that chatbots and self-service websites sacrifice security in favor of convenience.

Many consumers expect that they will become less and less likely to reach another person when they dial customer service. 31% of UK consumer respondents predict an increase in digital and automated self-service solutions will occur in the next half-decade, so there will be fewer service representatives answering the phones. 26% believe tomorrow's customer service functions will be evenly split between individuals and digital systems.

Just as new technologies like chatbots inspire worries, so too do new methods for payment. While 'traditional' online and in-app shopping are familiar and perceived to be safe, less than one in every three British consumers feels confident in buying a product or service over social media. Comparatively, less than 10% of U.S. respondents feel very confident about their data security when buying a product or service over social media, according to a survey we conducted in August.



81% of consumers worry that chatbots and self-service websites sacrifice security in favor of convenience

Varied Beliefs

PCI Pal's consumer surveys revealed that there's little consumer agreement about the best ways to interact with a business, which indicates that an omnichannel approach may be the most appropriate strategy for attracting the greatest variety of customers. The British results to a question about preferred ways of asking a product question indicate this. Nearly a quarter of respondents (23%) said they'd like to chat online with a real person, while a further 18% like talking to an operative on the phone.

So instant digital communication is the preferred way of interacting with businesses? Not so fast — 16% of respondents like to email questions and wait for a response, while a further 18% say they get answers by going to a branch or other physical location. Consumers have varying levels of comfort with digital and in-person interactions, and successful businesses should provide options that cater to all approaches, allowing consumers to interact via their channel of choice.

Trust and Convenience are Key

How do people want to make payments online? In the United Kingdom, nearly half of consumer respondents (48%) said online payment via a payment link was their preferred way to pay; 16% said they liked paying over the phone with a digital assistant, while 15% like reading their payment information to a live agent.

When asked why they chose their payment methods, 42% said they liked their method because "it feels secure or safe," 40% because they believe it's more convenient, and 34% because they think it's "trustworthy". In short, respondents tended to weigh both convenience and security when transacting. A payment link generated by a Secure Payments Provider is both convenient and secure; calling up a digital assistant is secure but not especially convenient. And if a caller has any doubts about contact centers, they're likely to consider reading their data over the phone to an agent both insecure and inconvenient.

Work Ahead for Social Media

Social media is widely used yet widely distrusted. Although social media commerce sales are projected to reach $605 billion by 2027, that staggering figure seems relatively low when considering just how ubiquitous social media has become since Facebook launched over fifteen years ago. And the ubiquity of social media makes these platforms uniquely attractive to hackers and bad actors. Early this year, LinkedIn suffered a hack that affected 700 million users. That's almost one in every ten people in the world. Is it any wonder that fewer than 7% of survey respondents feel "very confident" about social media purchases?

Roughly 70% of consumers claim that they'll avoid shopping at a particular store for a few months when there's a major and well-reported data breach. This trend might prove to be even more problematic for social media companies, since consumer sentiment is already so low that major firms have begun filling user feeds with defensive messaging. A massive data breach is always devastating to a business and to some of its users, but when consumers don't give firms the benefit of the doubt, the reputational and financial damage could prove even more extreme.

CONTACT CENTERS: REPORTS FROM AGENTS AND MANAGEMENT

Contact centers and their agents have endured a great deal since the advent of the coronavirus pandemic, but PCI Pal's research demonstrates just how successfully they have operated. While many people may not want to dial in to a contact center, the vast majority of people believe that they are safe and reliable.

In the United Kingdom, two-thirds of respondents expressed confidence that contact centers handled credit card data and other personally identifying information in a safe and secure way. The majority thought that security was as good or even better than it was five years ago, suggesting that they believed that contact centers had persevered through COVID without any loss of efficiency. Barely one in every ten (11%) respondents said that they were not confident in contact center security. In the United States, to compare, 61% of respondents felt 'very confident' to 'somewhat confident' that contact centers could handle their data in a safe and secure way.

General Confidence

Customer confidence about contact center responsibility and safety was mirrored by contact center professionals. While some operations may be happier and more efficient than others, most contact centers seem to have adopted security protocols and best practices that leave their employees with little doubt that the business is functioning as it should.

In the PCI Pal survey, 78% of American contact center professionals rated their confidence in their organization between 7 and 10 on a ten-point scale. British contact centers were similarly optimistic, with 76% expressing confidence in their organizations. Just 10% of American and 7% of UK respondents scored their organization between 1 and 4 on the ten-point scale. The vast majority of contact center professionals, both agents and management, believe their organization is doing the right things and heading in the right direction.

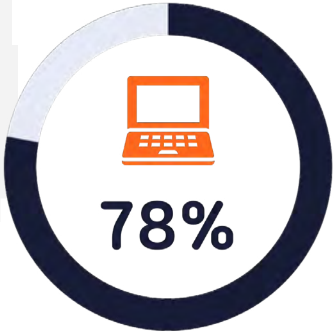
Historically, contact centers could function as a venue for fraud when customers read credit card information over the phone. Whether there was an unscrupulous agent in the contact center or a malicious third party listening in on the call, communicating payment data was fraught with risk. Today, the situation has improved. 75% of American and 72% of UK contact center professionals were confident that callers were not asked to read their personal payment information to agents. Just 11% of American and 12% of UK respondents expressed a serious lack of confidence in their institutions' handling of payment data.

New Risks

Although contact center agents and management are, by and large, confident about their organizations' security and policies, the survey suggested that there is ample room for improvement. Some of the obstacles that contact centers face stem from the unusual work situations that the coronavirus imposed, while others reflect weakness in policies, training, or technology.

More than half (52%) of British and American contact center survey respondents believe that working from home has increased the cyberattack risks that centers face. This makes intuitive sense: However, tech-savvy a person may be, they're unlikely to have enterprise-grade security on their home networks. And, especially at the beginning of the pandemic, many workers may have been logging in to work from personal computers that wouldn't be cleared for professional use in less urgent times.

Worries about security grew more prevalent as our survey moved higher up within contact center organizations. Agents were least likely to worry about remote-work security dangers; just 41% observed or predicted an increase in attacks. However, 56% of their managers and team leaders noticed or anticipated such problems, and a staggering 78% of senior management believed that remote work increased the risk of attacks. While agents may not have extensive knowledge of the threat landscape, the management teams with increased access to attack data are worried.



78% of senior management believe that remote work increased the risk of attacks

The perception gap between management and agents warrants further industry reflection. If, as many predict, some forms of remote work are here to stay, it is essential that leadership convey the seriousness of risks that hackers and identity thieves continue to pose.

Clear communication is essential for employee buy-in. Ensuring that the team, as a whole, recognizes a threat is the first step to neutralizing that threat.

The Future of Personal Service

While the news of customer confidence is heartening, there are more challenges ahead. At present, 54.9% of contact center professionals believe that technology adoption will thin their numbers over the next five years. As the number of agents decreases, however, so too may public confidence in an organization's service.

Senior management in contact centers, however, has a slightly different perspective. While organizations will continue to deploy new and improved technology to streamline processes, improve consumer experience, and automate rote tasks, it does not follow that there will be a decrease in personalized human-to-human contact. 34.2% of surveyed contact center management expect an increase in personal service.

Whether the next five years ultimately show an increase or a decrease in person-to-person interaction in contact centers, management must balance security and technology. Almost half of contact center respondents believed that an increase in automated technology deployment corresponds to an increase in organizational vulnerabilities that could lead to a cyberattack. Managers are even more wary: More than seven in every ten managers worry that new digital tools introduce potential security liabilities.

Internal Concerns

While two-thirds of consumers expressed confidence in contact center security and trustworthiness, the professionals who work in those centers often have serious concerns. Many American center employees complained of limited data security training — this is especially worrying given the pace at which hackers, scammers, and other bad actors devise new ways to attack systems. Problems identified by contact center respondents included limited training, out-of-date technology, and poor leadership.

The Training Gap

In the United States, 53.8% of contact center professionals who had worries about security cited poor or infrequent training as a major risk factor. In other words, less than half of American contact center employees believe they have received sufficient support in a central aspect of their job! It's clear that more and better training is needed.

53.8%

OF CONTACT CENTER PROFESSIONALS
have worries about security citing poor or infrequent training as a major risk factor

British professionals were markedly more optimistic: Only 40.6% of respondents worried that training was infrequent or poorly implemented. While both British and American centers need improvement in this area, the substantial Transatlantic gap in employee confidence is suggestive. Perhaps there are British training procedures that deserve further uptake in the United States?

Another possible explanation for the gap between American and British respondents may have to do with legislation. Although the United Kingdom exited the European Union in early 2020, a version of the General Data Protection Regulation (GDPR) remains in effect. That means that there are stricter training and security rules in place in the U.K. than exist in most American states. European laws, including British laws, tend to prioritize individuals, rather than businesses and corporations.

It's not just laws that may affect this. In Europe, there's also a stronger security culture in general: Americans are sometimes less cautious and more trusting with their data. When you employ a credit card to pay your bill at a restaurant in the United Kingdom, you're likely to do so from a portable payment device brought to your table. In the United States, more often than not you surrender your card to the server, who takes it away and returns it to you after running it through a payment reader elsewhere.

Leadership and Initiative

Although more than half of American respondents suggested that poor training was a serious problem, contact center professionals were less likely to attribute these problems to poor leadership. Just over a third of respondents (35.4%) claimed that weak leadership and direction about data security rules and processes constituted a major cause for alarm. Perhaps some respondents do not mentally link 'security procedures' and 'leadership'? If that is the case, the contact center leadership shouldn't just redouble its security training efforts. It should also emphasize to agents and lower-level management that security begins at the top and is a major leadership priority.

New Problems with Old Technology

Poll results make it clear that infrastructure and technology investment will be key to security in the months and years to come. 35% of the respondents who worried about aspects of their organizations' security cited legacy technology as an area of concern.

In some cases, organizations may have made an initial investment in tools, but failed to follow up and implement new, improved, or more secure products. After all, deploying new tools and training staff on new programs takes time, energy, and initiative. It's often easier to leave a legacy system in place — at least until that legacy system plays a part in a breach or other failure.

In addition, there may be a few contact centers that have neglected security best practices like running hardware and software updates. To take just one recent example from consumer electronics, any Apple product user is potentially vulnerable to the Pegasus hack. When contact centers fail to update systems, servers, and workstations, they may leave their systems wide open for an enterprising hacker.

Post-COVID Readiness

Some previously secure workplaces may have to relearn the best practices for safe operations in a post-coronavirus world. At the beginning of the pandemic, many contact centers switched to a completely remote structure and trained staff in the use of newly created remote access systems. These new systems were devised on extremely short notice by development teams that themselves had to work remotely. While many organizations deployed systems that met or exceeded the performance of pre-existing 'in office' solutions, the ad-hoc nature of the new systems' creation and implementation meant that flaws and gaps were more likely to go unrecognized and unrecorded.

As unpleasant as it is to admit, the unique circumstance of the coronavirus pandemic also gave cover to bad behavior by contact center agents. While contact center management should — and usually does — assume that agents are scrupulous and professional, there are occasionally dishonest employees. When operations run on-premise, traditional monitoring tools may have been enough to deter bad agents, who are thankfully rare..

Descoping tools like DTMF (Dual Tone Multi Frequency) Masking or speech recognition, remove temptation by ensuring that information like credit card data goes direct to the Payment Service Provider without ever moving through a contact center.

CLOSING THOUGHTS

The payments, security, and compliance industry, like so many others, has experienced epochal change over the past two years. Some changes, like the move to remote work on the part of many contact centers, seem likely to make the industry more accommodating, flexible, and appealing. Other changes, like the increase in automated digital assistant technology in contact centers, have left professionals and consumers alike with mixed feelings and lingering doubts.

PCI Pal's research of American and British consumers and contact center professionals reveal an industry in flux.

Consumers on both sides of the Atlantic are, by and large, confident that their data remains safe when they interact with large organizations or with contact centers. At the same time, they're willing to punish businesses that suffer breaches by withholding their wallets. It's clear that consumers don't see data breaches as something that just happens to an unfortunate company. Rather, these consumers interpret breaches as acts of neglect on the part of the breached business. Most of the time, organizations are compromised when external bad actors encounter internal failure.

When asked how they prefer to interact with a business, consumers were mixed. While many consumers prefer to ask questions via a phone chat with a real person or a live chat with a real operative via a website, some consumers prefer to email questions or to chat with a bot.

At present, there is no one-size-fits-all solution for business-customer interaction, so it makes sense for businesses to prioritize an omnichannel approach — and to ensure that all those points are secure.

Security remains a top-of-mind concern for consumers. When asked why they preferred to pay via a certain method, like a payment link, two extremely frequent answers were convenience and perceived security. Businesses looking to boost online conversions ought to consider the best ways to combine the twin goals of security and convenience.

Consumers have a mostly positive perspective of the organizations that store or transmit their personal details, although there are some exceptions to the general rule. Perhaps the most striking finding is how few people feel comfortable making social media-assisted purchases. Although social media is ubiquitous, feelings towards it tend to be ambivalent, and trust in it tends to be low. Recent events like the LinkedIn hack of 700 million records are unlikely to have improved the situation for the various social media firms.

Contact center professionals, like hundreds of millions of other people around the world, have seen their working lives radically disrupted since March 2020. Given the social change and technological advances they've witnessed, it's no surprise that some wonder what the future will hold. Because chatbots and digital assistants have become so familiar in everyday life — think of Alexa or Siri — and because they now play roles in contact centers, some workers worry that there will be fewer contact center positions available for humans five years from now.

Both consumers and their management team are more likely to demand a personal conversation in contact center interactions, perhaps because of their own knowledge of the industry and belief in the use of humans to handle these inquiries over digital assistants. Technology certainly has its place in these environments, to make the lives of contact center professionals easier, but it cannot replace the human experience.

While the vast majority of contact center professionals believe their organizations have complied with data security measures, the occasional doubts and concerns that they express deserve serious scrutiny. It's possible that some organizations saw security flaws introduced in the rapid switch from in-office to remote work; these issues must be identified and addressed. Other problems do not originate with the ongoing global struggle against the coronavirus. Some professionals worried that internal policies were unclear or outdated, others that training was too infrequent or too brief to fully prepare agents for their job. A final issue that contact centers must consider is the role of legacy technology in their operations. While old systems are familiar and new systems may be perceived as being difficult or costly to implement, in the end, the advantages of up-to-date systems far outweigh any misconceptions and disadvantages.

> "Fraud will always be present, and though attacks by governments on major criminal rings can scatter or shut down a large volume of fraud, they don't make the issue disappear. In 2022, it's time to get serious about cybersecurity - there's no longer an excuse."
>
> **- Geoff Forsyth**, CISO | PCI Pal

2021 has been a strange and often difficult year. Whatever challenges, opportunities, or surprises 2022 brings, PCI Pal will be ready to assist.

For more resources, visit our Knowledge Center.

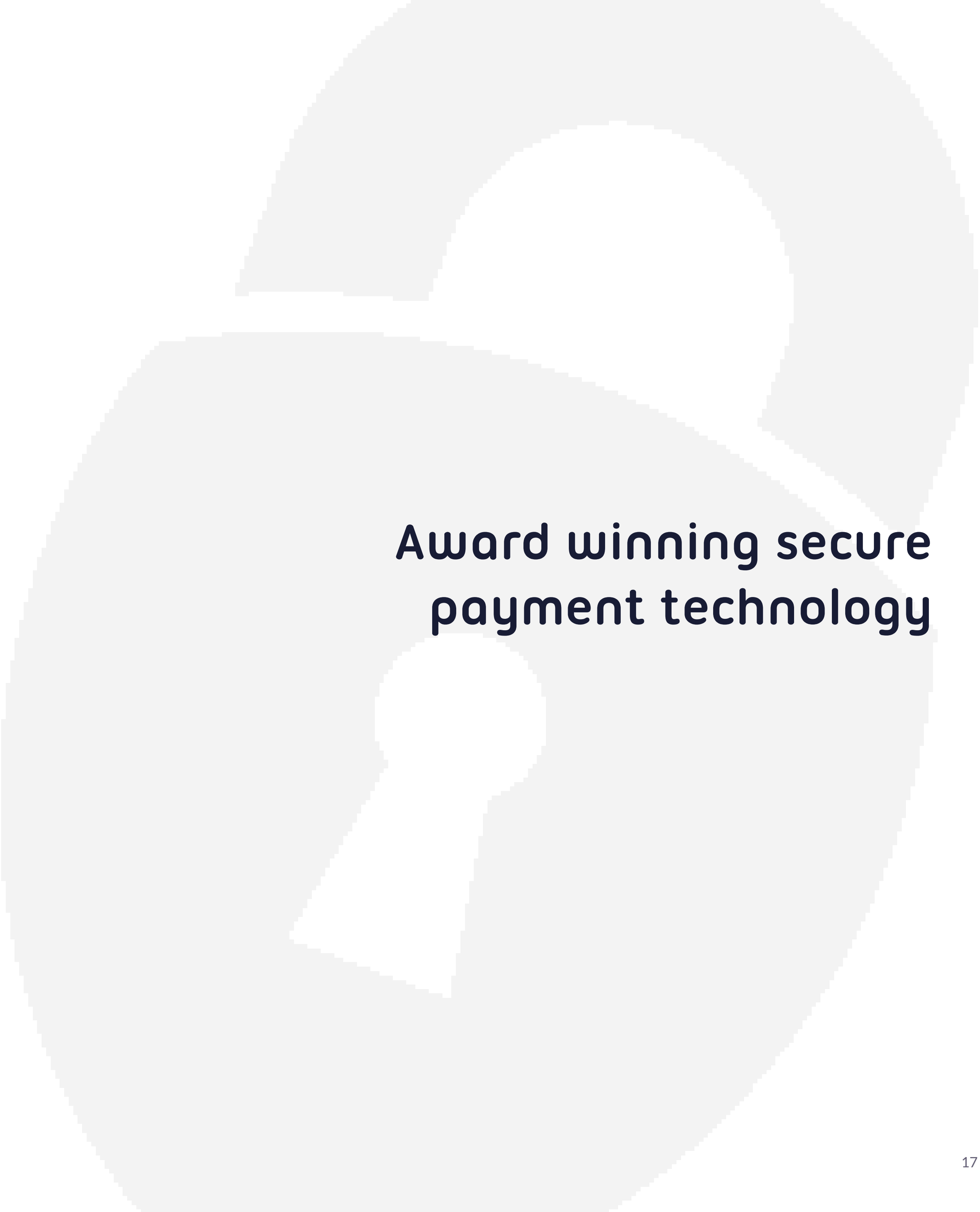
GET IN TOUCH

U.K. ☎ +44 207 030 3770

U.S. ☎ +1 866 645 2903

✉ info@pcipal.com

www.pcipal.com



Award winning secure payment technology

pcipal®

Award winning secure payment technology

www.pcipal.com