THE STATE OF DATA SECURITY IN CONTACT CENTERS

Analysis by

semafone®
securing data · protecting reputations

Contents

INTRODUCTION

With data breaches and cyberattacks occurring almost daily, organizations are looking to strengthen their data security practices to better protect customer data and avoid the reputational damage of an embarrassing public data breach.

Yet, one area of vulnerability is often overlooked when it comes to protecting data: the contact center. Since the widespread adoption of the EMV chip card, fraudsters have been shifting their focus to card not present (CNP) channels, such as contact centers – often deemed "low-hanging fruit." And, with personally identifiable information (PII) – including credit and debit card numbers, sensitive authentication data (SAD), social security numbers (SSNs) and more – regularly flowing through their IT environments, contact centers are especially attractive targets. To gain first-hand insight into the state of data security in the contact center, Semafone conducted an anonymous global survey of contact center agents across multiple industries, gathering more than 500 responses.

EXECUTIVE SUMMARY

This survey shows that a concerning number of contact centers continue to rely on outdated, risky practices for customer interaction, data collection and fraud prevention. For example, more than 70 percent of agents still require customers to read payment information aloud over the phone, despite available technologies for more secure data transmission. At the same time, a disconcerting number of agents have been approached directly by company insiders and/or outsiders to share customer information.

Survey findings emphasize the urgency for contact centers to secure all sensitive data and reduce the risk of brand-damaging data breaches. Current security measures, such as the use of clean rooms (no writing utensils, paper, phones or bags) and checkpoints for agents are not enough. While there is reason to believe that not all agents have fraudulent intentions, it is important to understand that it takes just one malicious person – coupled with poor data security – to send an organization into a downward spiral.

Recommended solutions for mitigating contact center security risks include: more robust incident management policies; proper access controls for computer systems; tokenization technologies that replace data with a meaningless equivalent; and dual-tone multi-frequency (DTMF) masking technologies that shield data from agents as customers enter it into their telephone keypads.

However, the best way to protect customer information, deter fraud and safeguard a company's reputation is to remove sensitive data completely from the contact center environment.

More than

70 percent

of agents still require customers to read payment information aloud over the phone, despite available technologies for more secure data transmission.

Key statistical findings from this survey include:

Contact centers still rely on outdated and risky data collection and customer interaction practices.

72%

of agents who collect credit or debit card information over the phone said they still require customers to read payment card numbers out loud, despite the readily available technologies that secure voice transactions

30%

of agents reported that they have access to customers' payment card information or SSNs on file even when they're not on the phone with the customer

Agents are experiencing and witnessing breach attempts from both insiders and outsiders, yet many do nothing to mitigate the risks.

7% of agents admitted that someone *inside* their organization had asked them to access or share customers' payment card information or other sensitive data

4%

said the same about someone *outside* their organization

9% said they personally know someone who has unlawfully accessed or shared customers' payment card information

42%

of agents who were approached said they did not report the situation

Contact centers aren't doing enough to protect customer data.

26%

of agents said they work in a contact center "clean room," which prohibits personal items and recording devices of any kind

38%

of agents are not allowed paper or pens at their work station

31% of agents are not allowed personal items or bags at their work station

28% of agents are required to pass through a security check before entering or leaving work

Industry and geographical trends are apparent.

0 European agents reported instances of outsiders approaching agents to share information – likely reflective of Europe's stricter governance rules

50% of agents in Central and South America have access to customer data when they aren't on the phone with the customer. These regions also had the highest number of requests to share data

35%

of agents in the Business Process Outsourcing (BPO) industry have access to customer information when they aren't on the phone with them; and **11 percent** said an insider had approached them to share customer information

The above findings point to increased risks due to outsourcing and offshoring, making strong data security even more important for contact centers with such business models.

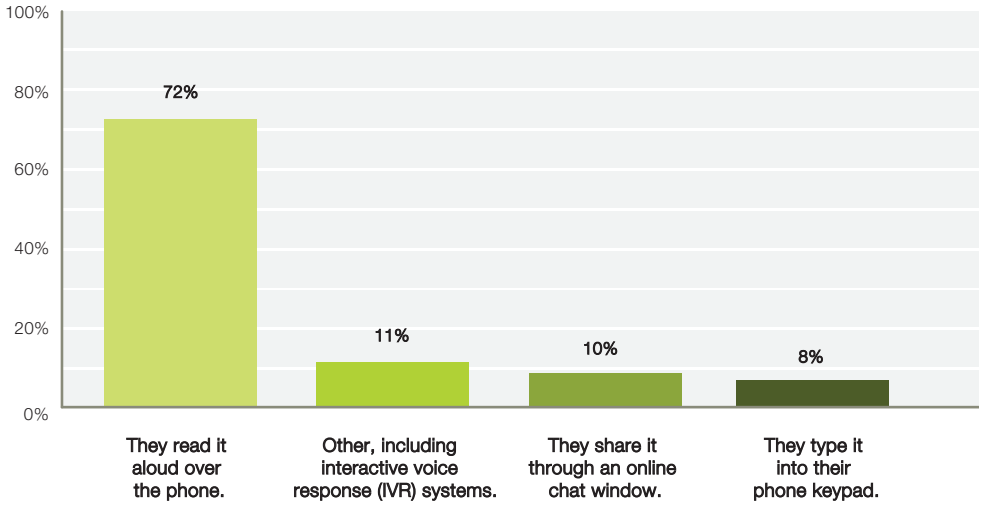
Data Collection and Customer Interaction

In response to this survey:

- **55 percent** of agents said that customers share credit or debit card information with them over the phone
- **36 percent** said that customers share that information via the Internet

Yet, some of the methods used by contact centers to gather customers' PII raise even greater concerns.

Figure 1. **How does the customer share their SSN or payment card information with you?**



Pause and Resume

When customers read their card numbers aloud, it creates additional challenges for organizations that record calls for legal, regulatory or quality assurance reasons. For example, the Payment Card Industry Data Security Standard (PCI DSS)[1], which provides guidelines for securing payment card data, prohibits the recording of sensitive authentication data (SAD), such as three-digit security codes, including CID, CVC2 and CVV2.

Many contact centers use a practice called "pause and resume" or "stop/start" to manually or automatically block payment card data from call recordings.

However, these practices create gaps in an organization's data management strategy:

1. If an agent forgets to pause the call, SAD and other PII may be inadvertently captured, putting the call recording back in scope for compliance purposes and leaving the information vulnerable should there be a data breach.
2. If an agent forgets to resume the call recording, vital information may be excluded that is needed to solve transaction disputes or support quality control.
3. With an incomplete call recording, a company may not be able to demonstrate compliance with industry or state/government regulations.

[1] "PCI Security Standards Council Document Library," Payment Card Industry Security Standards Council (PCI SSC): https://www.pcisecuritystandards.org/document_library

Reading Numbers Aloud

Seventy-two percent of agents who collect credit/debit card information or social security numbers (SSNs) over the phone said their companies still require customers to read payment card numbers aloud (Figure 1). This poses numerous security and compliance risks, as the information is exposed to the agent on the line, as well as nearby eavesdroppers. The information could easily be copied down for fraudulent use.

Sharing Data Through an Online Chat Window

Ten percent of agents said they capture customer information through a chat window. Although data is not verbalized in these cases, many of the same challenges experienced with live caller-agent engagements exist:

1. The contact center agent is still exposed to sensitive data through the chat window.
2. The merchant must prevent the storage of data on the desktop computer, CRM system and the webserver that hosts the chat application in order to secure the payment.
3. The contact center must implement an efficient, accepted and appropriate method to encrypt the payment session within the chat engagement.

The problem lies in the fact that basic chat functionality is just an “instant messenger” program that was not designed for encryption. While there are chat applications that offer secure connections, extra data protection measures are required, such as pre-exchanged passwords and security keys.

Using Interactive Voice Response (IVR) Systems

Eleven percent of agents said that they use “other” methods of collecting payments, including interactive voice response (IVR) systems. These automated telephony systems interact with callers to shield PII from agents, but they create their own set of issues. Without an agent on the line, customers often don’t know how to correct miskeyed information, which can result in ended calls before the transaction is complete. This poor customer experience can impact important contact center metrics like first contact resolution (FCR) and average handling time (AHT). Additionally, by having the customer hang up prematurely, the organization loses a potential sale.

Entering Data into the Telephone Keypad

Eight percent of agents said customers provide information by typing it into their phone keypad. This approach may involve using dual-tone multi-frequency (DTMF) masking secure payment technologies. DTMF masking solutions allow customers to directly enter payment card numbers into their keypad. Neither the agent on the line nor anyone listening to the call recording can decipher the numbers, as the DTMF (keypad) tones are masked with flat tones, and PII or payment card data never enters the contact center IT infrastructure.

Breach Attempts & The Threat Landscape

While contact center data security threats come in many shapes and sizes, most can be categorized as "insider" or "outsider" threats. The survey indicated that both types of threats are prevalent in the contact center, and that a concerning number of agents have been involved in some way.

Insider Threats

Company insiders account for approximately

50%

of security incidents[2], and more than

7,700

insider incidents (277 with confirmed data disclosures) were reported in 2016 alone.[3]

Suspect 1: Opportunistic Oscar,

The Tempted Temp

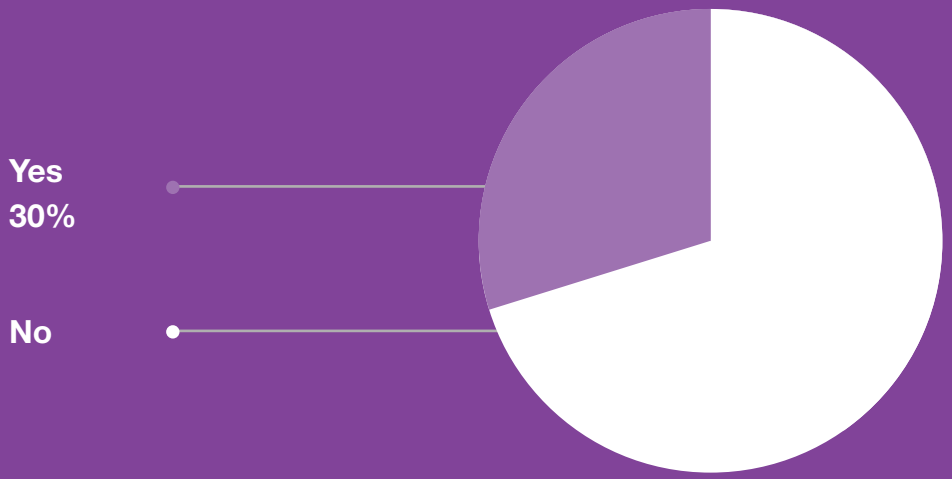
The situation: To accommodate high-volume periods like Christmas or sale days, contact centers frequently hire temporary or seasonal employees. These staffers can pose an added insider fraud risk, whether due to lax employee screening practices or a lack of loyalty to the employer.

The crime: Oscar lands a temporary position in a retail contact center to make some extra money during the holiday season. After taking a few calls, he realizes that customers are reading him their credit card numbers without hesitation. Thinking no one will notice, Oscar starts writing down callers' card numbers and is even successful in obtaining some CVVs and expiration dates. As a temporary employee with no loyalty to the company, he thinks he has very little to lose. Oscar goes home with his newfound information and begins his online shopping spree.

The lesson: Whether or not Oscar gets caught, this situation demonstrates that it can take just one agent to jeopardize customer data. It also shows the importance of investing in more thorough data security processes – for example, shielding payment information and other PII from agents. Relying on recruitment protocols to weed the "good" agents out from the "bad" is not enough, especially when it comes to temporary employees.

[2] "World's oldest hacking profession doesn't rely on internet," by Maggie Overfelt, CNBC, May 13, 2016: http://www.cnbc.com/2016/05/13/a-surprising-source-of-hackers-and-costly-data-breaches.html
[3] "2017 Data Breach Investigations Report," Verizon: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Figure 2. **Do you have access to customers' SSN or payment card information on file even when you're not on the phone with the customer?**



Unnecessary Access to Data

Thirty percent of agents said they have access to customers' SSN or payment card information on file even when they're not on the phone with the customer (Figure 2). This means that customer information is not only available to "rogue" agents for malicious use, but is also susceptible to a data breach due to accidental or negligent behavior. For example, an agent may open a phishing email or plug in a thumb drive that's infected with a Trojan. Or, an agent could forget to log out of his or her desktop, leaving sensitive information exposed to prying eyes.

Suspect 2: Unfortunate Ursula,

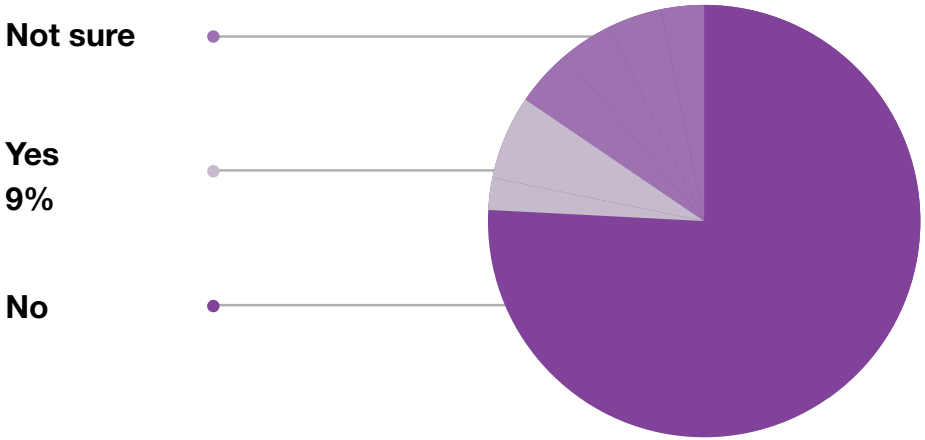
The Credulous Clicker

The situation: Not all fraudsters are malicious. Even the most trustworthy employee can accidentally expose sensitive customer data, especially if the data resides within the contact center environment.

The crime: Ursula, a diligent customer service representative, is responding to customer emails, resolving complaints, answering questions and facilitating account changes. She comes across an email from a customer claiming to have received a damaged product, including a photo in an attached file as evidence of the damage. Ursula clicks on the attachment, which installs a malicious worm that spreads across the contact center's IT network, stealing customers' data. Once the virus infection is detected, the company makes front page news for suffering a major data breach. In the coming weeks, the company's stock prices drop and customers take their business elsewhere.

The lesson: To prevent the damage caused by a well-intentioned employee who falls victim to a targeted outsider attack, businesses must properly train their staff on the dangers of phishing and social engineering tactics. Contact centers should educate their employees on what to look for and what to do in such a situation. A combination of staff training and removing sensitive data from business infrastructure is crucial.

Figure 3. **Do you personally know anyone in your industry who has accessed or shared customers' payment card information when they're not supposed to?**



The survey findings highlight many illicit behaviors that are contributing to the increasing insider threats posed to organizations.

Unauthorized Access to and Sharing of Data

9% of contact center agents surveyed said they personally know someone in their industry who has accessed or shared customers' payment card information without authorization (Figure 3). Similarly, **7 percent** said they had been asked by someone inside their organization to access or share customers' payment card information or other sensitive data (Figure 4). **Two percent** said that they had been offered a payment to share this information.

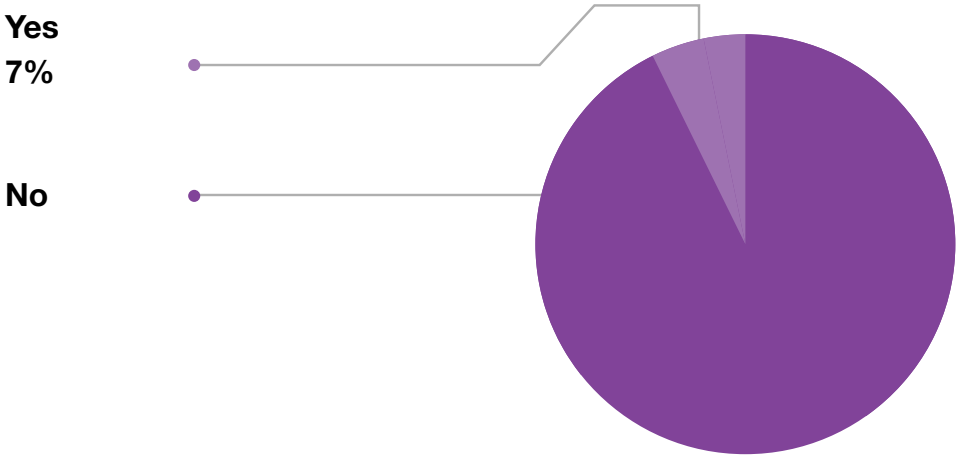
Suspect 3: Disgruntled Daisy,
The Vengeful Victim

The situation: Although an agent may not be the mastermind behind a fraud operation, there are others inside the contact center's organization who may have malicious intentions. The catalyst for a data breach can come down to three simple things: a disgruntled employee, an accomplice with access to customer data and a bribe.

The crime: Daisy has worked at a contact center for 10 years and is dissatisfied with management. While she no longer directly works with customers, she has many colleagues who are employed as agents. Daisy offers to pay one of her colleagues $100 in exchange for customer payment card data. She justifies her fraudulent activity as compensation for her years of being underpaid and underappreciated. From her perspective, the theft won't hurt anyone, as most customers have fraud insurance.

The lesson: One angry employee can put all customers in danger of identity theft and fraud. Companies must keep PII out of the contact center environment if they are to also keep it out of the hands of malicious insiders.

Figure 4. **Has anyone inside your organization ever asked you to access or share customers' payment card information or other sensitive data?**



Despite these alarming findings, it is important to note that most contact center agents are actually good, honest and trustworthy people. The adage, "good guys must be right every time, but the bad guys only need to be right once," applies here.

With poor data security, it takes just one successful hacker or fraudster to offset the positive work of a typical agent.

Outsider Threats

Rogue agents and malicious insiders are not the only ones putting customer data at risk. Research shows that outsider security threats have increased by as much as 300 percent[4].

Figure 5. **Has anyone outside your organization ever asked you to access or share customers' payment card information or other sensitive data?**

Four percent of agents confirmed that someone outside the organization had asked them to access or share customers' payment card information or other sensitive data (Figure 5). In addition, **2 percent** said they had been offered a payment to share or to allow an outsider to access this information.

Although **4 percent** is a relatively low figure, it is likely that there is a significant number of incidents that go unreported or unnoticed. The use of social engineering tactics makes it particularly difficult to detect attempts to manipulate agents into providing customer information. In fact, **60 percent** of enterprises[5] fell victim to at least one targeted social engineering attack in 2016, and financial accounts were breached in **17 percent** of those attacks.

Suspect 4: Scheming Steve,

The Secret Cyber-man

The situation: Employees aren't the only ones who expose or access sensitive data, whether maliciously or accidentally. Contractors, IT support and other third parties who regularly come in contact with agent desktops also pose an often-overlooked risk.

The crime: Steve is an IT contractor who is learning how to hack into IT systems for fun. His intent is mostly harmless. However, one of Steve's clients is a contact center for a bank. Realizing how much personal information the contact center holds, Steve decides to put his hacking skills to the test. While fixing an agent's computer, Steve discretely inserts a keyboard, video and mouse (KVM) switch into the back of the machine. These unassuming devices allow users to control multiple computers remotely. From his home computer, Steve can now hack into the contact center's network and access customer accounts. With this information at his fingertips, he could easily steal thousands of dollars.

The lesson: Any data stored within the contact center infrastructure is vulnerable, and hackers will take advantage of every opportunity to access this data illegally. The most effective way to protect this data is to ensure it's not stored in the first place.

[4] "Malicious outsider data breaches up nearly 300%," by Bob Violino, Information Week, March 30, 2017: https://www.information-management.com/news/malicious-outsider-data-breaches-up-nearly-300

[5] "60% of enterprises were victims of social engineering attacks in 2016," by Roi Perez, SC Magazine UK, November 30, 2017: https://www.scmagazineuk.com/60-of-enterprises-were-victims-of-social-engineering-attacks-in-2016/article/576060/

Small Numbers Add Up to Big Risks

While the aforementioned statistics are seemingly small numbers, when applied to the larger contact center agent population globally, the risk is significant.

Consider this: there are approximately 2.2 million contact center agents in the U.S. alone[6]. Based on the survey findings, it is possible that close to 150,000 active agents in the U.S. have been asked to share sensitive customer and payment data by others within their company; and more than 85,000 agents may have been approached by an outsider to share information.

Moreover, the damage resulting from a successful breach can be devastating. The average consolidated total cost of a single data breach is $3.62 million, according to IBM's 2017 Cost of a Data Breach Study[7]. The report highlights that each lost or stolen record containing sensitive and confidential information costs an organization an average of $141. This figure takes into account more than just financial losses and customer compensation, but also the reputational damage, legal fees, auditing services and more.

The average consolidated total cost of a single data breach is $3.62 million, according to IBM's 2017 Cost of a Data Breach Study.[7]

---

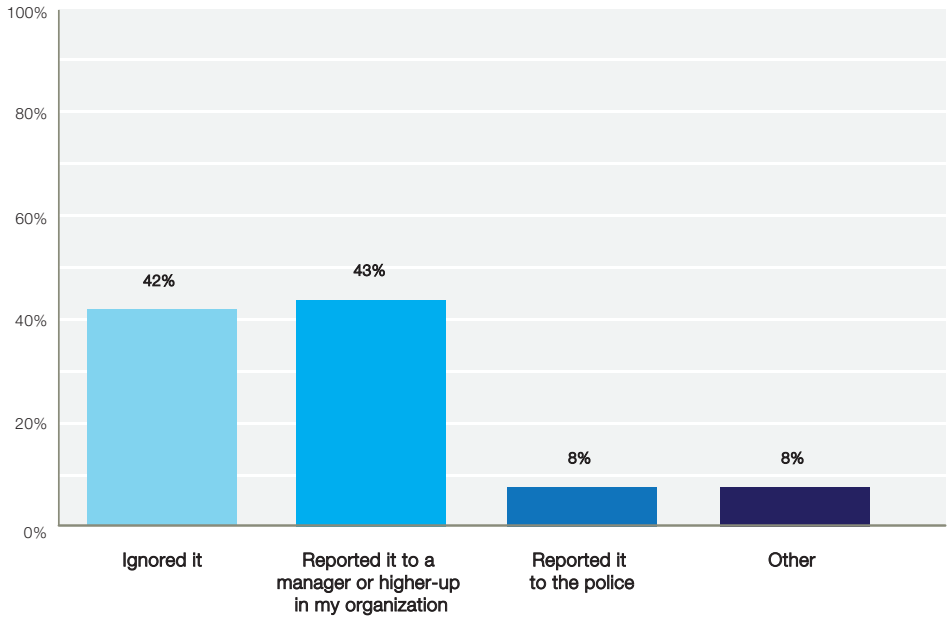
[6] "How Big is the U.S. Call Center Industry Compared to India and The Philippines?" by King White, Site Selection Group, February 17, 2015: https://info.siteselectiongroup.com/blog/how-big-is-the-us-call-center-industry-compared-to-india-and-philippines

[7] "2017 Cost of Data Breach Study," IBM: https://www.ibm.com/security/data-breach/

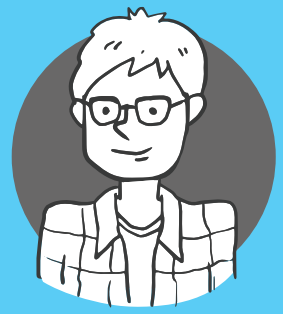
Handling Breach Attempts

Of agents who have been asked to share data, only **43 percent** notified a manager or supervisor of the situation and **8 percent** reported the attempt to the police (Figure 6).

Figure 6. **If you experienced a potential breach by an insider and/or outsider, what did you do about the situation?**



Alarmingly, **42 percent** said they did not report the incident, indicating that a sizeable number of data breach attempts go unnoticed by an organization.



Suspect 5: Conniving Carl,

The Contract Cleaner

The situation: When sensitive data is stored in the contact center, it is susceptible to being stolen by anyone who has easy access to the IT system – even someone as unassuming as a maintenance operative or a cleaning crew.

The crime: Three times a week, Carl works as a janitor at a large corporate building where he has unrestricted access to every floor and office. One of the tenants is a contact center and Carl learns that the computer system stores large amounts of customer information. While cleaning the office, Carl slips a thumb drive containing malware into several computers. Over the course of the next week, the malware captures detailed information of all customer transactions, including payment card numbers. Carl returns the following week to remove and collect the thumb drives, which have gone completely unnoticed.

The lesson: Third parties with access to the contact center pose significant risks when sensitive data is available. Removing the data from the business and IT environment can avoid this risk and protect customers' information.

What Data is Most at Risk?

Of the agents who had been approached by someone inside or outside their organization to share customer information:

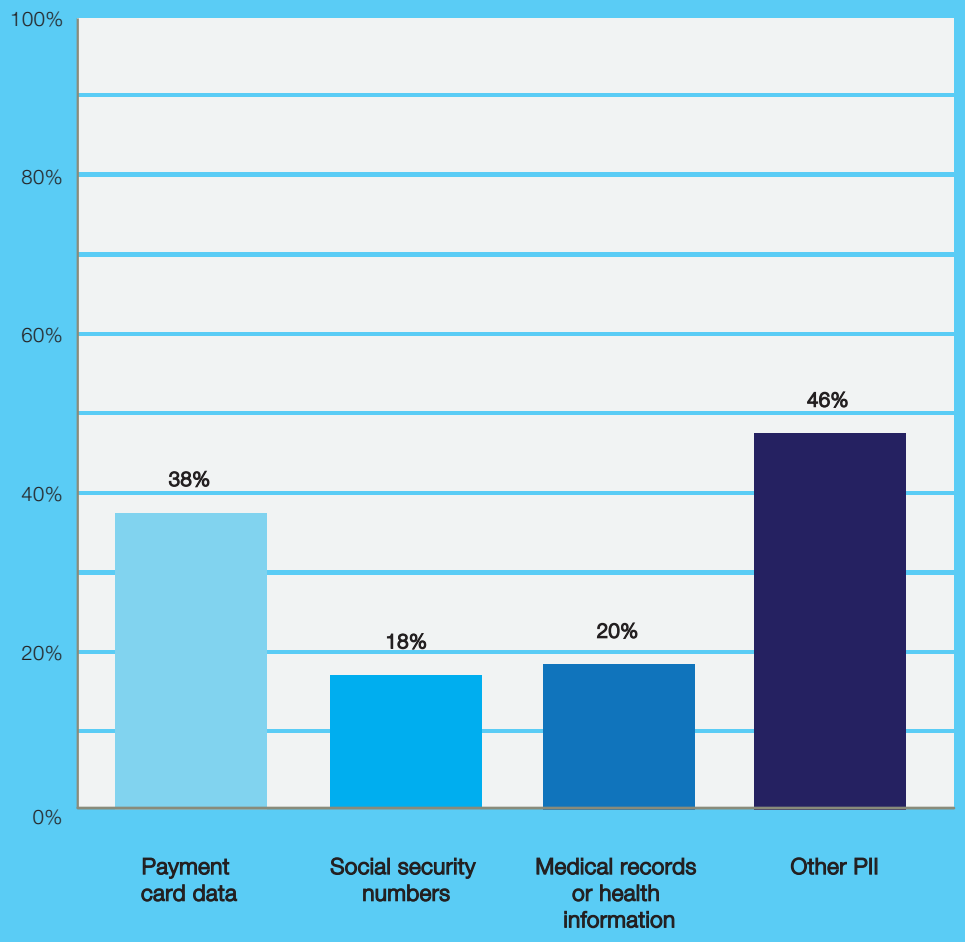
38% were asked for payment card data

20% were asked for medical/health records

18% were asked for SSNs

47% said they were asked for "Other PII," which includes customer names, contact information, etc. (Figure 7)

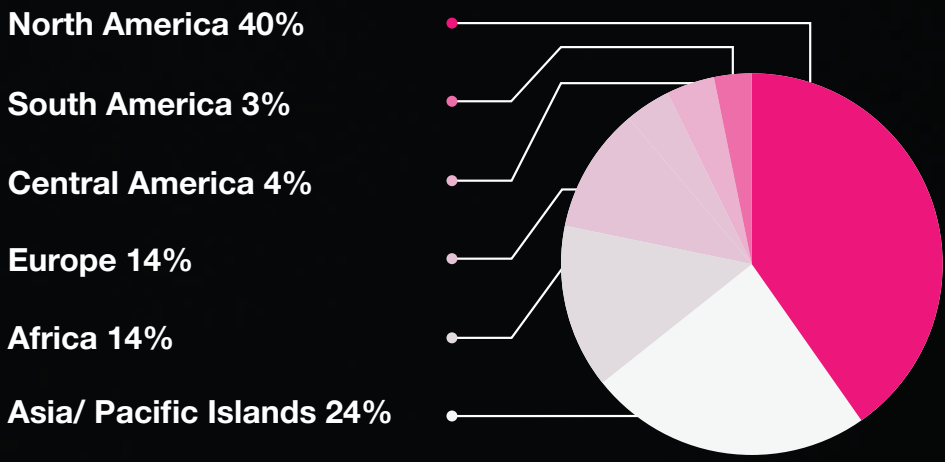
Figure 7. **What type of information were you asked to access or share?**



Geographical Variations

The survey gathered responses from contact center agents around the world. Participant breakdown is as follows (Figure 8).

Figure 8. **Which region do you live in?**



Some Significant Geographical Statistics Emerged:

North America had the highest percentage of agents whose customers provide payment card information and SSNs over the phone **(70 percent)**. It also showed the third-highest percentage of agents who have access to customer information when they are not on the phone with them **(31 percent)**.

In Central America and South America, **50 percent** of agents said they had access to customer SSN or payment card information when they aren't on the phone with the customer. This is a matter of concern, given that the agents in these areas also had the highest number of requests from both insiders and outsiders to share customer data. Central America also had the highest percentage of agents who were offered a monetary bribe to share sensitive data **(10 percent)**.

Asia reported a high threat level and ranked third in percentage of agents approached by insiders and outsiders to share customer information **(13 percent)**. However, only **35 percent** of agents in Asia said they take customer payment information and SSNs over the phone.

Europe emerged with the least apparent risk, with the lowest percentage of agents who said they have access to customer information when they aren't on the phone with the customer **(16 percent)**. Europe was also the only region to report **zero** instances of outsiders approaching agents to share information.

Is Europe Leading the Way?

There are a few factors that may explain Europe's all-around low percentages. First, European regard for PCI DSS is growing[8], and organizations are becoming more aware of the repercussions of non-compliance. This is true not only with PCI DSS, but also with the Information Commissioner's Office (ICO) in the U.K. and the pending European Union General Data Protection Regulation (EU GDPR). As a result, many European companies have stricter top-down governance, including the enforcement of the principle of least privilege. This protocol states that users should only have access to systems and tools when they are required in order to perform a job. Therefore, it follows that Europe has the lowest percentage of agents with access to customer data when they are not on the phone with that customer.

Secondly, Europe doesn't handle SSNs, which are often used as an easy way to begin an identity theft attack in the U.S. This makes other PII less attractive to harvest. Thirdly, in some parts of Europe, card numbers aren't necessary to complete transactions. For example, Germany and Sweden use pay-by-bank methods, which mean that callers simply are not sharing permanent account numbers (PAN) or PII.

Lastly, regarding Europe's zero instances of outsiders approaching agents to share information, hackers employing social engineering tactics have likely discovered that European agents have far less access to sensitive PII. Any available access is carefully tracked and monitored, making this approach less fruitful and can assist forensic investigators identify which records have been targeted, thereby identifying the fraudulent agents.

[8] "Why PCI Security Standard Adoption Is Growing in Europe," by Mathew J. Schwartz, Bank Info Security, July 14, 2016: http://www.bankinfosecurity.com/blogs/europe-pci-security-standards-adoption-increasing-p-2181

GEOGRAPHIC FINDINGS: SUMMARY

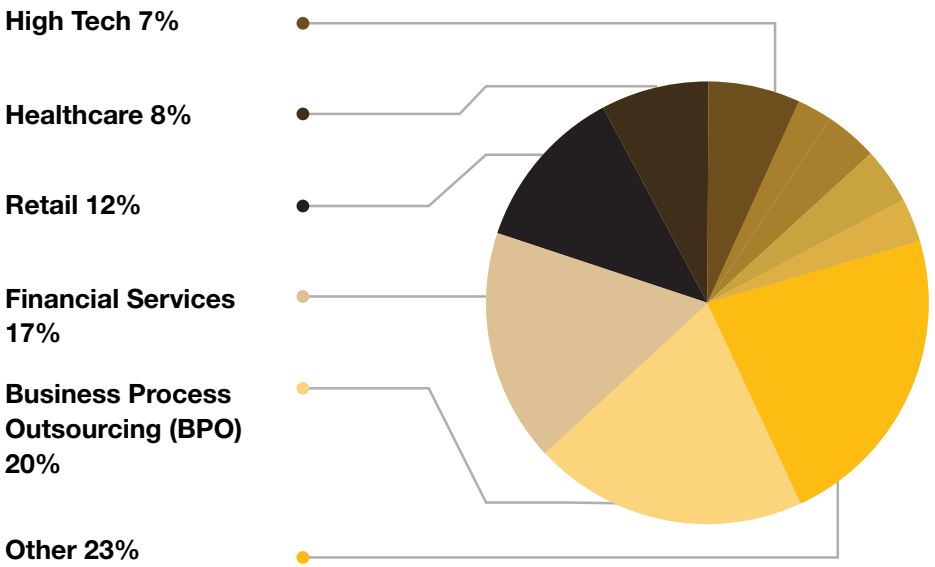
The use of risky, outdated contact center practices – including having customers read payment card numbers aloud – is common around the world. However, Europe's stricter governance rules put the region ahead of others in terms of effective data security practices. North America, with the highest percentage of agents taking PII over the phone, shows opportunity for risk and can learn from Europe's best practices. Central and South America need to take further measures to restrict agent access to PII, as they had the highest percentage of agents with access to customer data when not on the line with the caller. These regions also showed the highest percentage of both inside and outside breach attempts.

The use of risky, outdated contact center practices – including having customers read payment card numbers aloud – is common around the world.

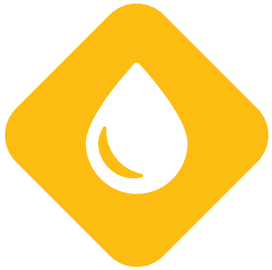
Industry Findings

In addition to a geographically diverse group of participants, this survey generated responses from contact centers in many different industries (Figure 9).

Figure 9. **What industry is your company in?**



Key Findings by Industry:



The Utilities industry not only had the highest percentage **(75 percent)** of customers providing SSNs and credit/debit card information over the phone, but also had the highest percentage of agents **(11 percent)** who said they personally knew someone who had unlawfully accessed customer information.

Business Process Outsourcing (BPO) was another industry with high percentages across the board. More than **35 percent** of agents said they have access to customer information when they aren't on the phone with them; **11 percent** said an insider had approached them to share customer information; **3 percent** had been offered a bribe; and **10 percent** said they personally knew someone who had unlawfully accessed sensitive data.

In the Hospitality industry, **42 percent** of agents said they have access to customer information when they are not on the phone; and more than **10 percent** of those agents had been approached by an outsider to share this information.

Despite the Healthcare industry ranking second in number of 2016 data breaches,[9] it was the only industry in this survey whose agents did not say an outsider had attempted to obtain customer information from them.

Agents in Government had the second-highest percentage of agents approached by insiders to share customer information **(9 percent)** and third-highest approached by outsiders **(5 percent).**

[9] "The ITRC 2016 Data Breach Report," Identity Theft Resource Center: http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

INDUSTRY FINDINGS: SUMMARY

Based on these survey findings, contact center data security issues span all vertical industries. The Hospitality, BPO and Government verticals ranked highest in the percentage of agents experiencing fraud attempts (from both outsiders and insiders), with Utilities following close behind. Most notably, the BPO sector consistently reported higher than average numbers in several areas of risk, including the number of breach attempts by outsiders and the number of agents who have access to data when they aren't on the phone with the customer. While outsourcing and offshoring can lead to cost savings, they come with significant, additional risks. In fact, research shows that poor outsourcing decisions cause **63 percent** of data breaches.[10]

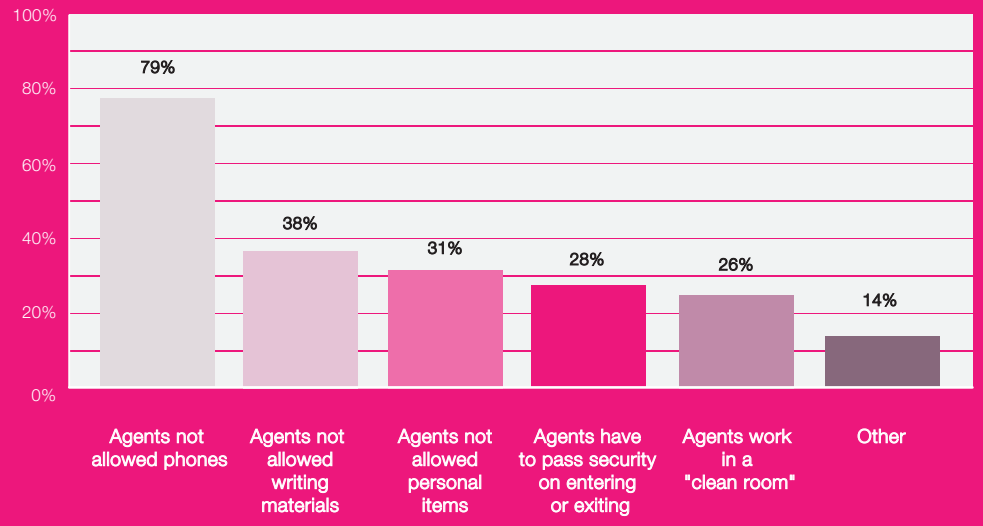
If outsourcing or offshoring are part of one's contact center strategy, good data security is even more important, as you cannot outsource the damage to your brand reputation in the event of a breach.

[10] "Bad outsourcing decisions cause 63% of data breaches," by Warwick Ashford, Computer Weekly, February 15, 2013: http://www.computerweekly.com/news/2240178104/Bad-outsourcing-decisions-cause-63-of-data-breaches

Security Measures: How are Contact Centers Currently Protecting Customers' Data?

To conclude this survey, participants were asked about the types of security controls their organization has in place to prevent contact center agents from taking customer data (Figure 10).

Figure 10. **What type of security controls does your organization have in place to prevent contact center agents from taking customer data?**



The most common security method encountered was prohibiting of cell phones at agents' work stations **(79 percent)**, followed by:

- Banning agents from having writing materials **(38 percent)**
- Barring personal items/bags **(31 percent)**
- Requiring agents to pass through a security scanner or checkpoint upon entering or leaving **(28 percent)**
- Working in a contact center "clean room," which forbids personal items and recording devices of any kind, as well as requiring strict security checks **(26 percent)**

With a turnover rate of up to 45 percent for agents in the U.S,[11] retaining employees is already a challenge for contact centers.

The Drawbacks of These Security Measures

Draconian measures to control the actions of contact center employees can be effective for protecting sensitive data, but can also negatively impact employee morale. In fact, they can raise operational costs and lead to increased staff turnover. Furthermore, if customer payment information is read out loud, agents are still able to hear it and are sometimes required to enter it into a computer. The information may also end up on a call recording, whether intentionally, as the result of human error, or due to a failure in the pause and resume system. Regardless of workspace restrictions, sensitive customer data still touches various CRM systems and desktop applications.

[11] "Understanding Call Center Turnover," by Ricardo Valente, Talkdesk.com, March 11, 2016: https://www.talkdesk.com/blog/understanding-call-center-turnover

How Contact Centers Can Secure Customer Data & Reduce Risk

It is impossible to predict and prevent every potential breach, but there are a number of steps contact centers can take to reduce risk and keep customer data safe. The following best practices will help mitigate many of the risks unveiled in the survey findings – including the use of outdated data collection practices, agent exposure to sensitive data, insider and outsider breach attempts and the use of draconian security measures:

1. Treat all data as toxic

With cybercriminals and fraudsters seeking a wide range of data (from credit card numbers, to birth dates, to SSNs) contact centers must treat all PII as toxic. The more information that is vulnerable in the case of a breach, the easier it will be for a criminal to steal a customer's identity, drain their bank account, access their private medical records and more. For the victim, resolving an incident of identity theft is especially distressing, expensive and time consuming.

2. Properly train (and vet) employees

Contact centers should take time to properly train and educate agents on the very real dangers of insider- and outsider-caused data breaches. For instance, they should create awareness surrounding social engineering tactics and advise agents to report suspicious activity to a supervisor. Also, hiring "good people" is not enough. Conducting thorough background checks, even for temporary employees, is a valuable step.

3. Implement an incident management policy

Contact centers should have an incident management policy and/or process in place, preferably as part of an Information Security Management System. It is wise to prepare for a worst-case scenario and have a documented Incident Response Plan that is tested at least annually.

4. Fight social engineering with tokenization

Humans aren't error proof, so contact centers should use technology to assist in the event of a social engineering attack. One ideal method is to use tokenization to replace data with a meaningless equivalent. Even if a breach is successful, the available data will be of zero value to the cybercriminal.

5. Enforce the principle of least privilege

When possible, use the principle of least privilege on computer systems. This will give employees the minimum level of access required to perform their job function at the appropriate time. So, if the agent doesn't need to view customer credit card data when a phone transaction isn't taking place, for example, they shouldn't have access.

6. Authenticate the user to authenticate the agent

This simple approach essentially prevents agents from having access to customer data until the agent has received the right data from the user. This means that until the caller has been successfully identified using the appropriate secure authentication approach, access to detailed PII is denied.

While incident management plans and employee training sessions are great, they only go so far.

Descope the Contact Center: They Can't Hack Data You Don't Hold

While incident management plans and employee training sessions are great, they only go so far. The crux of the situation is that sensitive data is being exposed to agents, held in various business systems and captured on call recordings – just waiting to be compromised. The only way to truly reduce risks is to remove sensitive data from the contact center environment, completely. After all, they can't hack data you don't hold. But, how?

DTMF Masking Technology

Using dual-tone multi-frequency (DTMF) masking technology is one of the most effective ways for contact centers to de-scope their environment (or, to significantly reduce the number of applicable PCI DSS controls). Such technologies allow customers to enter payment card information and other PII directly into the telephone keypad. DTMF tones are masked with flat tones, so the agent on the line, the call recordings and any eavesdroppers are unable to decipher the numbers. The agent can remain in full conversation with the customer throughout the call, assisting with any issues and completing wrap-up tasks, thus enhancing the customer experience, and even improving first contact resolution (FCR) and reducing average handling time (AHT). Once information is entered into the telephone keypad, it is sent straight to the appropriate third party (like a payment processor), bypassing the contact center's infrastructure altogether.

Problems Solved by Descoping

By descoping the contact center environment, organizations can solve the challenges underscored by the survey results. Descoping enables the following:

Agents are no longer exposed to sensitive data, nor do they have access to customer PII when they are not on the phone with them. This reduces risks associated with “rogue” employees and social engineering tactics. Moreover, when approached by insiders or outsiders to share customer information, agents are unable to oblige.

Customers do not need to read their card numbers aloud and have full control over inputting their data.

Sensitive data is not stored in the contact center infrastructure, rendering hacking attempts (by both insiders and outsiders) useless.

PCI DSS compliance is dramatically simplified, allowing organizations to cut costs and focus on business as usual (BAU).

There is no need for clean rooms or excessively stringent security measures that jeopardize employee morale. A better working environment means happier, more productive employees and reduced turnover, which can translate to a better bottom line.

CONCLUSION

This survey confirmed that many contact centers still use inadequate, outdated practices when capturing, processing and storing payment card data and other PII. Complicating the situation, agents are exposed to this information and are even experiencing breach attempts, as insiders and outsiders approach them to illicitly share sensitive data.

With the growing threats to data security, contact centers simply cannot wait around for an incident to occur before taking action. The only way to prevent costly data breaches and protect customers' information is to remove sensitive data completely from the contact center's business infrastructure. It takes just one agent mistake, one rogue employee, one phishing email or one fraudulent phone call to instigate a data breach that adversely impacts an entire enterprise, its customers, its reputation and its bottom line. Organizations must protect themselves from a multitude of threats, 100 percent of the time, while an attacker must only succeed once. **So why wait to address contact center security? It's not worth the risk.**

semafone®
securing data · protecting reputations

About Semafone

Semafone is your contact center data security and compliance expert. We work closely with enterprises around the world to remove sensitive data from IT and business networks – protecting your customers and your company reputation, while simplifying compliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS). Our award-winning, patented data capture method allows contact center agents and customer service representatives (CSRs) to securely capture personal information including payment card data, bank account details and social security numbers over the phone using dual-tone multi-frequency (DTMF) masking technology. Unlike interactive voice response (IVR) systems, agents remain in full voice communication with the caller as they enter their numbers into their phone keypad, ensuring a positive customer experience.

By conducting this survey of more than 500 global agents, we hope to raise awareness about the risks inside and outside today's contact centers – a part of virtually every business – and create a greater sense of urgency among the contact center community for securing their data…and securing it *now.*

+1 888-736-2366

info@semafone.com

www.semafone.com

@semafone

Google+

LinkedIn

745 Atlantic Avenue, Boston, MA 02111, USA