OVER THE PHONE CREDIT CARD FRAUD:

A PCI Compliance Guide for Business and Government

ivrnet

The pace of business today is real-time and instant. Customers want products and services the moment they feel they have all required information to make a decision. Consumers expect secure transactions processed and authorized in real-time while they're on the phone. This presents a security threat. Many businesses, municipalities, and organizations do not realize the risks involved when collecting sensitive payment card information over the phone.

In this guide, we explore security issues specific to over the phone credit card payments, to help your company

- *Combat the risk of credit card data breaches*
- *Decrease costs and responsibility of securing this data*
- *Gain greater customer service agent efficiencies*
- *Earn greater consumer confidence*
- *Protect your reputation*
- *Continue to offer the convenience and immediacy of taking credit card payments over the phone*

What you'll find in the guide:

- *Impact of card not present fraud*
- *What does PCI compliance mean to my industry?*
- *Maintaining compliance with over the phone transactions*
- *How over the phone credit card fraud happens*
- *Business benefits of compliance*
- *Eliminating risk through descoping*
- *Case study for municipalities*
- *What to look for in secure solutions*
- *Best practice resources*

IMPACT OF "CARD NOT PRESENT" FRAUD

What is card-not-present (CNP) fraud and how does it affect businesses and government entities?

CNP includes over the phone payments, internet and e-commerce transactions, and mail-order transactions where the cardholder does not physically present the card to the merchant.

In Canada, 2011 financial losses to Canadians for CNP fraudulent transactions totaled $259 Million with the average dollar loss per transaction $644. Moreover, the one year rate of growth of these losses over 2010 losses was a stunning 47%.

According to a U.S. Payments Forum report, CNP fraud is currently the most prevalent type of fraud reported in countries that have migrated to EMV chip, and it continues to increase. With the exponential growth of e-commerce, many are struggling to keep up with security standards in place to prevent CNP fraud.

The impact of this growing area of credit card fraud impacts a variety of businesses and government entities. It is no longer the banks or the credit card companies that bear the risk or responsibility for security. Breaches and theft of cardholder data affects everyone, including individuals, businesses, and government—

- *Customers lose trust in merchants or financial institutions*
- *Individuals are at risk for bad credit scores and identity theft*
- *Merchants lose credibility and future business*
- *Government agencies risk painful audits and recovery costs*
- *Risk of lawsuits, class-action lawsuits, and settlement payments*

Maintaining PCI Compliance is good business and it is necessary to protect yourself, and your customers, from a wide array of risk. Many of our clients, from the automobile industry to Homeowner Associations and government agencies, still rely on taking payments over the phone. This type of CNP transaction is vulnerable to fraudsters in a variety of ways.

HOW DOES PCI COMPLIANCE APPLY TO MY INDUSTRY?

Let's begin with a working definition of PCI compliance. What does it mean and who needs to worry about it?

PCI stands for Payment Card Industry. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard which aims to protect data and reduce credit card fraud.

Credit card brands mandate the PCI Standard and the Payment Card Industry Security Standards Council administers it. **How do they validate compliance? Here are the options:**

- *An external Qualified Security Assessor (QSA)*
- *A firm-specific Internal Security Assessor that creates a Report on Compliance for organizations handling large volumes of transactions*
- *Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes*

Does your business accept credit card transactions over the web? *Over the phone? Is e-commerce part of your future? If you accept or process payment cards, the PCI Data Security Standards apply to you.*

ivrnet

MAINTAINING PCI COMPLIANCE WITH OVER THE PHONE TRANSACTIONS.

We hear this common question from our clients: “Can I still ensure security if I take credit card payments over the phone?” As discussed in the introduction, card not present transactions pose a serious risk for businesses and individuals. What does it take to ensure your business can still offer over the phone payments? In this video, a PCI-Qualified Security Assessor discusses compliance challenges for taking customer credit card information over the phone through manual, hand-keyed methods.

What will they examine for PCI Compliance? It involves looking closely at all of the human processes and technology processes your organization is using.

- *A close examination of employees (training, background checks)*
- *Is the technologist AND the technology compliant?*
- *What are the security parameters, antivirus, patches, network system, firewalls?*
- *A close examination of call agents or third party call centers, and their processes and technology parameters.*

ivrnet

PCI Security Standards Council recommends the following for a strong data security foundation:

- *People: Hire people you can trust. Work with partners and vendors who understand payment data security.*
- *Process: Follow good data security policies and practices. Make it a priority in training and in daily operations.*
- *Technology: Use the right technology and implement it correctly.*

Later in the guide, we will take a deep dive into some technology solutions that can help mitigate the risk of human error and fraud as it relates to CNP and over the phone transactions.

But first, let’s look at some common phone-based credit card fraud scenarios.

OVER THE PHONE CREDIT CARD FRAUD: HOW IT HAPPENS.

Telephone-based credit card transactions present two opportunities for fraudsters. They are a source from which to harvest sensitive data and a target where these stolen cards can be used. Both of these risks are increasing as criminals target telephone-based systems as the weak link in the payment chain: While chip and pin protect brick-and-mortar establishments and online transactions can be secured using 3D Secure (e.g., Verify by Visa and MasterCard Securecode), phone payments remain vulnerable.

The very fact that an agent has access to sensitive credit card data by hearing it spoken by the customer in order to enter it into their CRM or ERP system (which then also stores this data), puts you at risk from fraud. This risk is extended if customer service calls are being recorded (e.g., for quality assurance).

These fraud risks should not be underestimated. PCI-DSS standards are meant to assess, prevent and manage these risks at the cost and responsibility of organizations.

Examples of fraud can be found in any industry sector.

In a case that caught public attention, a customer service agent was convicted of stealing credit card data and plundered thousands from their credit card accounts.

Another case involves call center employees selling information from thousands of credit card and bank accounts for small amounts of money.

In another occurrence In October 2011, a merchant's server was hacked and infected with a virus which was undetected for 2 ½ months during which sensitive data was emailed to the hacker as it was processed, enabling duplicate credit cards to be produced.

RISKS OF HUMAN ERROR WHEN TAKING PAYMENTS OVER THE PHONE

- *Untrained employees*
- *Unethical behavior*
- *Accidental privacy breaches - losing data, computer left unattended*
- *Unethical behavior of people in proximity to your employees/customers*

In putting together this guide, employees at Ivrnet offered up their own stories of over the phone credit card fraud that had happened to them. In one case, it was a hotel and card information was spoken over the phone. The credit card information was stolen and used, but traced back to the hotel as the source of the breach.

Another example was from an employee who could no longer use a particular food delivery service. The service was known for breaches, hacked accounts, and fraudsters ordering deliveries on other people's accounts and getting free meals. Now her credit card company won't allow transactions for this service.

What's the solution?

For brick and mortar businesses, there are approved PTS Devices that provide strong protection for payment data and take advantage of EMV chip, mobile and contactless technologies.

How can you identify a secure technology solution for processing payments over the phone? The most secure method of taking payments over the phone is simply not to manually enter, store or manage sensitive data at all. The best way to comply with PCI Data Security Standard is to remove the payment element from the call entirely.

Technology solutions, like Ivrnet Safepay, obtain real-time authorizations securely using a simple automated service, transmitting via traditional telephone lines over the Publicly Switched Telephone Network (PSTN).

WHAT ARE THE BENEFITS OF COMPLIANCE WITH PCI SECURITY STANDARDS?

Compliance with PCI-DSS can bring major benefits to organizations of all sizes, while failure to comply can have serious and long-term negative consequences.

Consumer Confidence

Compliance with the PCI-DSS means that your systems are secure, and customers can trust you with their sensitive credit card information. Consumer confidence is a growing issue for businesses and entities who need to take payments online and over the phone. Consumers are increasingly more concerned and fearful to give anyone their personal and financial information. Identify theft, credit card fraud, and a variety of scams have made the average person wary of giving out their credit card number to an individual over the phone.

Compliance improves your reputation with acquirers and payment brands—the partners you need in order to do business.

Prevent Breaches

Compliance is an ongoing process, not a one-time event. Maintaining compliance helps prevent security breaches and theft of credit card data—not just today, but also in the future.

Opportunity for Efficiencies and Improvement

Compliance may provide some indirect benefits, such as having a basis for a corporate security strategy and identifying ways to improve the efficiency of your IT infrastructure. Often this process involves working with a technology partner who is experienced at solving the problems you're facing, improving systems with automated solutions, and making your systems more secure and more efficient.

Avoid Costly Disasters & Fees

Not being compliant can be disastrous. Account data breaches can lead to catastrophic loss of sales, relationships, reputation and depressed share price. Possible negative consequences also include lawsuits, insurance claims, cancelled accounts, credit card issuer fines and government fines.

ELIMINATING RISK THROUGH DE-SCOPING

Removing sensitive credit card data from your infrastructure using a secure, third-party solution eliminates your organization's risk of fraud associated with telephone credit card information by moving it out of scope from the Payment Card Industry Data Security Standards (PCI-DSS).

If your customers do not read out their payment information over the phone, your agents cannot hear it, cannot write it down and cannot pass it on to anyone else. If agents don't enter sensitive payment information into their desktop, this too takes both the desktop and the network out of scope for PCI-DSS.

PCI-DSS has 222 compliance requirements for processing, transmitting or storing credit card information. Implementing these controls require significant investment in the development of new policies, tools and manual procedures, and also to document them for evidence purposes. Each control and its environment incur its own cost and the cost of a security audit.

As a result of the complexities surrounding compliance, organizations are finding it more cost-effective to eliminate credit card information altogether and partnering with a trusted third-party solution. The following case study shows how a government agency was able to solve risk issues and boost productivity through de-scoping.

MILESTONE:

30,000+ reports a month

1.5 million reports filed
since 2006

ivrnet

Case Study

The Government of Alberta has mandated the de-scoping of all credit card data as an effective method of improving efficiency, lowering costs, eliminating risks and safeguarding its reputation on behalf of Albertans. Ivrnet is proud to partner with the Government of Alberta employing Ivrnet Safepay for an agency serving local citizens who qualify for low income support. These individuals login to a secure website or call into IVR services when they need to report income, change of circumstance, and other reports.

Ivrnet has worked with this agency to set up a secure, automated system for users to report via the web or phone. The system uses an auto-process or a post-verification process. This means it's easier and more secure for citizens to report their sensitive personal information, and case workers get to spend more time with individuals rather than manually processing reports.

Prior to automation, reports were filed via mail or phone, and a manual verification process. Now after a 10 year process, about 60% of citizens are using the online system and 40% are using the phone system.

By working with a trusted technology partner, the government agency fulfilled their compliance obligations while increasing efficiency and improving customer service.

SECURE SOLUTIONS FOR OVER THE PHONE PAYMENT PROCESSING

Today's society is real-time and instant. Customers want products and services the moment they feel they have all required information to make a decision. Consumers expect secure transactions processed and authorized in real-time while they're on the phone.

Given the option between an easily accessible telephone call and the cloud/internet, many people still prefer to pay for products and services on the phone with a customer service agent, rather than being directed to a self-serve website. Not everyone has access to a laptop or computer with internet access, but nearly everyone has access to a phone.

Some customers may feel that organizations divert to a website for the organization's benefit and efficiencies. As a result of this frustration, funneling prospects or customers to a payment website may result in the loss of immediate sales and customer churn.

Security with Telephone Transactions

Customers understand and appreciate the enhanced security of their sensitive credit card information not being accessible to the customer service agent or recording facilities. As consumers become more aware of call agent fraud, recorded conversations that include spoken credit card information, and fraudsters who may be listening in to conversations, they are looking for the most advanced security measures to ensure they will not become a victim.

One solution is a system that allows the consumer to enter their own credit card number into the phone without having to speak it aloud to an agent.

Your system should be capable of retrieving and processing sensitive credit card data over the phone, while satisfying all PCI-DSS requirements—notifying both the Customer and the Agent about the result of a transaction.

Maximize Agency Efficiency

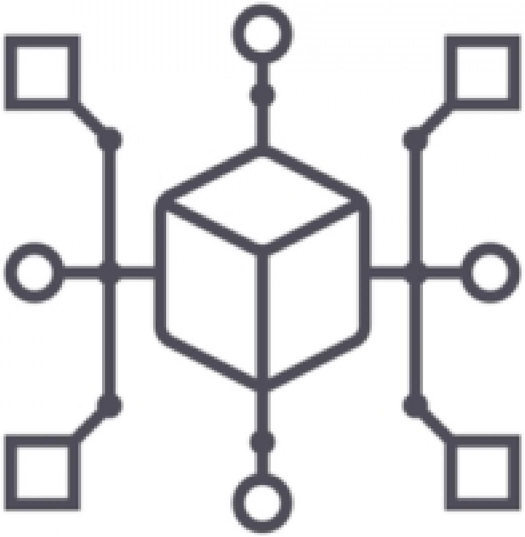
Customer service agents often spend time waiting for customer credit card data, manually entering numbers and expiration dates—a growing list that now usually includes credit card number, expiration date, security code, zip code, billing address, etc.

Example:

In addition to offering secure over the phone payment processing for your customers, you can offload some of the call agent work when you use a secure technology solution. **Here’s how it works:**

- *Customer service agent takes order and gets all of the information from customer*
- *Final step is to transfer the customer to Safepay for the customer to enter payment card information*
- *Agent is free to take calls from other customers waiting in the call queue*
- *Both agent & customer are notified that the payment went through successfully*

We have estimated that this type of solution will save organizations $33.13 per work day per Agent in salary costs. This is based on an Agent with a base salary of $35,000 completing 52 transactions per seven hour shift with an average of 8 minutes per transaction. Safepay transactions take a maximum of 90 seconds to complete. This results in a 23 per cent savings in both costs and efficiency.



Customized Integration

The over the phone security solution you choose must be able to integrate with your existing payment and CRM/ERP system. This results in a better user experience for both the Agent and the Customer as information does not have to be entered into both the existing system and an external payment terminal (e.g., a website provided by a bank, their service providers, or credit card issuers).

At Ivrnet Inc., we are experts in the automation of information collection and maintain the highest level of security and compliance. You can be confident that services provide a good user experience that is simple to use, logical and intuitive. We have proven this expertise in numerous projects and products in a variety of industry sectors and are continuously improving our knowledge by analyzing our customer’s needs and feedback as well as doing active research.

BEST PRACTICES RESOURCES

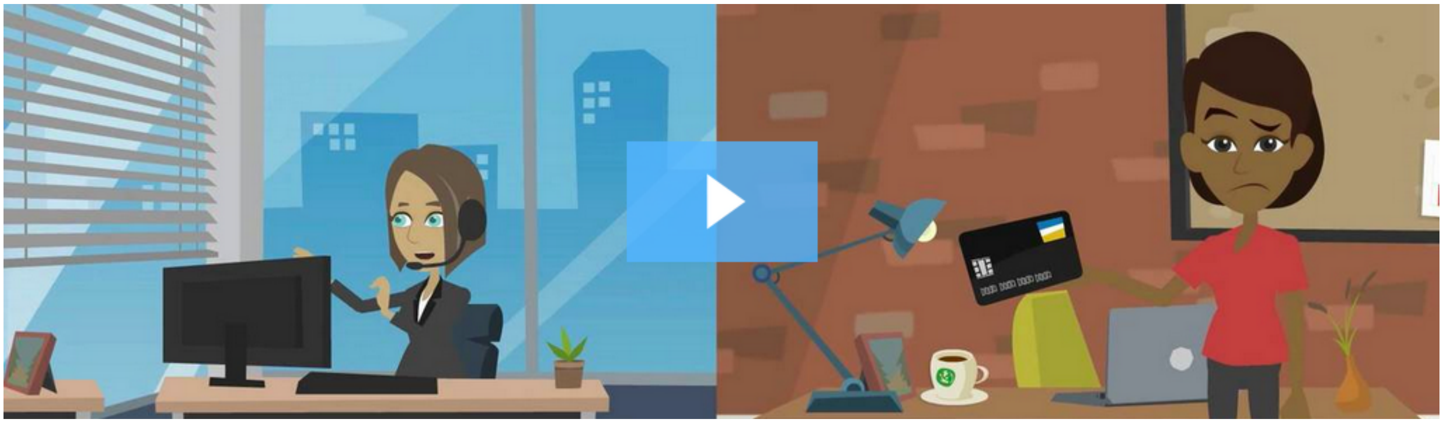
The following resources contain extremely detailed information about PCI compliance best practices for call centers and others taking payment card information over the telephone:

Report: PCI Security Standards Council Information Supplement: Protecting Telephone-based Payment Card Data https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf

Website: PCI SSC Document Library https://www.pcisecuritystandards.org/document_library?document=pci_dss_v2-0#pci_dss_v2-0

Article: PCIComplianceGuide.org “How Does Taking Credit Cards by Phone Work with PCI?” https://www.pcicomplianceguide.org/how-does-taking-credit-cards-by-phone-work-with-pci/

Learn More About Ivrnet Safepay



ivrnet