Sample On-Line ordering security plan. Reprinted with permission from Julie Valdez, President, Pacific First Computers jvaldez@p1c.com. Several included names and phone numbers have been deleted.

The following agreement was provided by Pacific First Computers in response to a solicitation in which the buyer contemplate using Purchasing Cards to place orders for products using the sellers on-line ordering web site.

Executive Summary

Pacific First Computers proposes to supply Buyer, with site standard Hewlett-Packard printers and peripherals as specified in the site standard table. Ordering would be accomplished through the use of Buyer's Purchase Cards (P-Card) in a secure web site environment. Pacific First Computers would be responsible for maintaining the web site, managing the transactions and keeping the pricing and product information updated.

Furthermore it would be Pacific First Computers responsibility to ensure that Buyer P-Card transactions were handled in as secure environment as possible. This includes our close management of authorized user name and password list, provide maximum user confidentiality and privacy, and maintain a mitigation plan should payment information be compromised.

1.0Security/Sensitive Data Plan

1.1On-Line Ordering Security

- Pacific First Computers agrees to work with Buyer to provide mutual security and safety in using on-line ordering.
- The order entry process will be secured by using SSL technology. Pacific First Computers will regularly monitor the security certificate.
- Pacific First Computers will not store credit card information, neither electronically nor by any other method.
- Pacific First Computers agrees to provide Buyer with a mitigation plan. That plan is in section 2 of this document.
- Pacific First Computers agrees with Buyer that only a limited number of people will have access to the ordering process, security arrangements, and user information.

- Buyer and Pacific First Computers agree that user access will be terminated on a timely basis when appropriate.
- Both Parties agree to share information between system administration or operation personnel which might affect the security or operation of this ordering agreement with respect to system security, virus concerns, scams, spam, fraud attempts, hacker attacks, firewall violation, and any other compromises as may be applicable.
- Pacific First Computers will never give nor sell personal or confidential information about Buyer personnel/company or Buyer's account to any third party not affiliated with Buyer's transaction except as required by law, or necessary to provide the services requested by Buyer, or as requested and authorized by Buyer to do so.
- Pacific First Computers agrees to ensure that users are not subject to spam, solicitations, advertising, or mailers of any type.

1.2 Privacy Policy

Pacific First Computers will ensure that maximum confidentiality and privacy is maintained at all times and to the greatest degree possible. The Buyer's company and account information is collected during the ordering process by e-WebCart.com. e-WebCart's system administrator, the owner of e-WebCart, and three individuals at Pacific First Computers will have access to this information. It is stored by e-WebCart for a period of 90 days, and managed by Pacific First Computers. Pacific First Computers can delete this information at any time based on Buyer's instructions. It is stored using 128-bit SSL encryption. EWebCart does not store credit card information.

The following is Pacific First Computers' point of contact information:

Primary Contract Administrator:
Account Manager

Secondary Contact:
President

Contact in President's Absence:
Account Manager

The contract would be administered from our Richland, Washington office. The primary method of communication for placing orders and confirming orders would be Internet e-mail to Ken Mannin. Mr. Mannin would also be the first point of contact for all customer support issues such as order cancellation, order changes, DOA products.

Buyer Business Information to Third Parties
Pacific First Computers is using two third party web companies under this contract: e-WebCart.com and iPayment Technologies. e-WebCart provides the secure shopping cart environment. This company will store the name, billing, and shipping address of the P-Card Holder. IPayment Technologies processes the credit card transaction. They will have access to the above information plus the credit card number and expiration date. E-webcart.com permanently deletes the credit card number and expiration date once the transaction is completed. Neither company will have the username and password information.

Security Technologies
Pacific First Computers employs the following security technologies under this contract: On the P1c.com site, where only the username and password are stored, Pacific First Computers employs the following security methods: Cisco 1720 Router with Firewall, and SNORT intrusion detection software. Any appearance of intrusion or attack is automatically flagged and our network administrator is notified.

Buyer Business Information Control
Buyer will control their business information and its removal from our database in the following methods: Pacific First Computers will delete a username and password within 24 hours of Buyer's written request. The P-Card holder's name, billing, and shipping information will be automatically purged from e-WebCart's server every 90 days or may be deleted as often as daily per Buyer's request.

Written request will be in the form of an e-mail from authorized Buyer representative to designated Pacific First Computers personnel.

1.3 Web Site Information

The following information will be requested from the P-Card Holder:

Username and Password:
The username and password list is stored on Pacific First Computers' web server. It is stored in an ODBE format accessed via an ASP page. Once this information is entered the P-Card holder is redirected to a new page. This has no bearing on the final transaction.

Quantities of catalog items:

These are not stored.

Billing address including, name, address, phone number
Shipping address including name, address, phone number
These are stored by e-WebCart, for a period of 90 days. The following parties will have access to this information: Pacific First Computers above designated personnel, e-WebCart system administrator, and the owner of e-WebCart.

Credit card number and expiration Date:
Humboldt Bank, and iPayment Technologies store these in an encrypted manner on a secure server for a period of six months.

E-mail address:
Stored by e-WebCart.com for 90 days or can be deleted daily. Pacific First Computers designated personnel, e-WebCart's system administrator, and the owner of e-WebCart will have access to this information.

1.4 Data Protection

The following tools will be employed to ensure that P-Card holder data is protected from loss, misuse, alteration, or theft:

Local Firewall and Intrusion Detection Methods
Pacific First Computers has in place a Cisco 1720 Router with Firewall software. In addition, we use the intrusion detection software SNORT to monitor our network. Any appearance of intrusion or attack is automatically flagged and our network administrator is notified.

At least two times per month we perform a remote penetration test to our own network from a Linux server sitting on the outside of our firewall. This scans for open ports and other vulnerabilities. A report is printed and given to the network administrator and the company president to review.

Log-In Access Control
P-Card holders must have a valid username and password to order products on-line from Pacific First Computers. The usernames and passwords are administered by Pacific First Computers. The password must be at least six digits in length and contain at least one special character. Passwords will be changed every six months.

Only designated Pacific First Computers personnel will have access to this information. Only authorized Buyer personnel may request Username and password updates.

The username and password are controlled by a session cookie, and will expire after 20 minutes of P-Card holder keystroke inactivity.

Secure Server
P-Card holder transactions take place on a secure server using Secure Sockets Layer (SSL) technology. SSL uses a private key to encrypt data being submitted from a browser before it is transferred over the Internet via the SSL. When the data reaches the SSL-enabled web server, it is decrypted. If the data were to be stolen during this transmission, it would remain unreadable.

Pacific First Computers will regularly monitor e-WebCart's security certificate to make sure that it is still valid.

Address Verification Service (AVS)
The Address Verification Service (AVS) is a fraud protection service that is built into the authorization process for non face-to-face transactions. When a P-card is keyed into the system, the address and zip code are sent along with the transaction data and compared against the address registered with the bank. A response code is sent back indicating whether the address submitted matches the information on file. Pacific First Computers is notified of the mismatch and at that point can contact the Buyer P-Card Administrator.

Transactions $5000 and over will not be processed until confirmed via a phone call to the Buyer P-Card Administrator or other designated individual.

Firewall
The next line of defense to maintaining data security (following SSL data encryption) is the Internet Firewall. Ipayment.com contracts with the highly regarded Network Services Provider, Genuity for their Managed Internet Security.

Genuity uses a firewall gateway service that restricts data communications to and from iPayment Technologies network. This service includes 24 X 7 monitoring, maintenance and response. The firewall is based upon the award-winning, market-leading Check Point Firewall-1, Site Patrol.

If Genuity detects an attack or threat to Ipayment.com servers, they immediately develop and transmit a DMZ specifically addressing this threat to ensure iPayment's network is continuously protected. Each threat response includes a description detailing the nature and severity of the threat, the risk it poses and what steps iPayment IT staff should take to ensure their network is protected.

It Genuity detects a threat that they deem serious; they will activate a choke hub. This is a device that sits outside the firewall and can be used to remotely shut down a particular network service that is under attack, an entire server, or the entire network.

Username and Password Storage

Pacific First Computers will store P-Card holder usernames and passwords only in an electronic method. They will be stored on our web server in an ODBE format accessed via an ASP page. Once this information is entered the P-Card holder is redirected to a new page. This information has no bearing on the final transaction. E-WebCart and iPayment Technologies will not have any way to access the usernames and passwords.

Secure Page Indicator

The security indicator will be a padlock in the lower right-hand corner.

Correcting, Updating, Deleting, Personal Data

This will be accomplished by sending an e-mail with detailed instructions to Pacific First Computers Account Manager. If this person is not available, Buyer will receive a return e-mail stating as such and redirecting them to the next available Pacific First Computers designated point of contact.

Pacific First Computers will require the e-mail to contain a digital signature. If this signature cannot be verified, Pacific First Computers will call Buyer before granting the request. Pacific First Computers will respond to all e-mail requests via e-mail.

2.0Mitigation Plan

Pacific First Computers does not store any Buyer order or payment information on our servers. However, our third party payment processing company, iPayment Technologies does store Buyer P-Card transaction information on their secure servers for a period of six months. Hence the need for mitigation plan.

Having stated the problem, and understanding the inherent risks, Pacific First Computers has developed a mitigation plan to minimize the effects of a breach, where a hacker was able to access Government Credit Card Accounts. In any case, Pacific First Computers will exercise the "Best Commercial Practices" to protect financial data, which is parallel to acceptable banking practices. Upon researching what the Federal Government expects, Pacific First Computers contacted the following salient resources:

(name deleted)
Card Technology Division
Department of the Treasury
Financial Management Services

(name deleted)
Applied Technology Division
Department of the Treasury
Financial Management Services

(name deleted)
Government Credit Card Division
Bank of America

The following Mitigation plan steps are based in part upon their recommendations and the "best commercial practices" to protect financial data.

Successful Attack
The following steps will take place in the event of an attack upon iPayment Secure Servers:

In the event of a successful attack, where data is actually compromised or stolen, Genuity immediately contacts the IT manager on duty at iPayment Technologies (contact Michael Stankowitz, iPayment's IT Manager). IPayment Technologies determines exactly what data has been compromised.

The following organizations are notified **immediately:**

- American Express, VISA, Discover, and MasterCard: with the list of stolen credit card numbers pertaining to their respective companies.

- The FBI Fraud unit

- IPayment.com merchants, including Pacific First Computers. Pacific First Computers provides iPayment Technologies a 24X7 phone number for this purpose.

- Pacific First Computers instructs our Webmaster to immediately shut down the on-line ordering process.

- If Buyer P-Card holder transaction information has been stolen, Pacific First Computers **immediately** contacts the 24X7 contact at Buyer with the list of compromised credit card numbers.

- If Buyer P-Card holder information has not been compromised but iPayment Technology servers have been successfully attacked, Pacific First Computers will still notify the Buyer and shut down the on-line ordering process.

- If necessary, or upon Buyer's request, Pacific First Computers will change to a different secure transaction processing company.

- Pacific First Computers has the ability to change third party transaction providers without changing our website or shopping cart program. It would take approximately 48 business hours for our company to change to a new secure transaction processing company. We maintain a current list of transaction companies compatible with our software in the event this needs to take place.

3.0Sample Invoices

Please find Sample Invoices attached.

Included are actual invoice samples and a sample automated e-mail order confirmation. Please note that we did not use a credit card to create these invoices. Should a P-Card holder place an order, “Payment Method” would state “Credit Card” instead of “Purchase Order.”

4.0 Value-added Services

Pacific First Computers will provide a minimum of the following value-added services to Buyer:

- Monthly transaction reports

- Quarterly meetings with Buyer authorized representatives to confirm pricing, confirm that best and most current product is being purchased, web site ease of use, etc.

- Transaction monitoring including fraud screening

- Local stock of at least one spare HP peripheral to be determined by Buyer.

- Pacific First Computers will pay all initial set-up fees and all monthly and annual fees associated with the on-line shopping cart and secure transaction-processing company.

- Pacific First Computers will provide prompt web site updates. We will provide same day updates for the following:
  Username changes, additions, deletions
  Product Price Changes
  Product Availability messages
  These updates will be made on the same business day if the request is received prior to 11:30 AM.

- Thumbnail photos and detailed product specifications can be added to the product descriptions.

- The secure shopping cart provided to Buyer will be exclusive for this contract. No other Pacific First Computers clients will have access to this same shopping cart.