Home Builders Association of Greater Cincinnati (HBAGC)
Credit Card/Bank Account Security Policy

Executive Summary

Vision and Philosophy

HBAGC puts securing our members' personal data as one of the organization's highest priorities. We understand that every time a member or customer provides us with credit card and bank account information, or other sensitive personally identifying information, they trust that we will protect it—and this policy is designed to ensure that this trust is not misplaced. The foundation of our information security program is a set of strong policies that are in balance with business operational needs.

Security Environment

HBAGC utilizes customer data to deliver products and services to our members. Accordingly, all member information to include cardholder data as well as other sensitive customer and company information, will be protected by all staff, contractors, partners and services providers in accordance with well defined policies and procedures.

HBAGC will operate on the security principle of "that which is not explicitly allowed is explicitly denied." Attempts by anyone to access, monitor, use or share information that is not explicitly allowed to them by our security program will be considered a security violation. Further, access to sensitive information will be permitted on a "need to know" basis, such that employees have access to only those data and systems required to perform their assigned jobs. We will deploy systems, processes, policies and training to protect our mission critical data assets and customer privacy. Most important, we will monitor and enforce compliance to our policies.

Vendor Management

Vendors, partners and other third parties will be required to comply with the same standards established for HBAGC staff. All vendors storing or otherwise accessing our customers' card holder data must provide proof of PCI DSS Compliance.

Sanctions for Policy Violation

Failure to comply with Security policies and guidelines may result in disciplinary action by HBAGC depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s). Each situation will be judged on a case-by-case basis. Sanctions may include termination of employment and / or referral for criminal or civil prosecution, warnings, or additional security awareness training. There is no requirement for advance notices, written or verbal warnings, or probationary periods.

Information Classification, Storage and Destruction

All HBAGC information is categorized into two main classifications: Public and Confidential.

Public information, such as advertising and marketing materials, is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to HBAGC.

Confidential comprises all other information such as sales data, customer addresses, employee files, etc, that should not be made available outside the company. A subset of Confidential information is "Critical Confidential" information, which should be restricted to "need to know" access only, such as trade secrets, financial, technical, and personnel information, and other information integral to the success of the company. Customer sales authorizations containing credit card numbers and cvv2 codes or bank account numbers (PANs), and PANs provided to employees in the course of entering a telephone transaction, fall into the "Critical Confidential" information category.

HBAGC personnel are encouraged to use common sense judgment in securing Confidential information to the proper extent. "Critical Confidential" information will be stored in a limited access area (i.e. locked file drawer or safe), and only those employees with a "need to know" will be provided access to that information. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

Under no circumstances is a CVV2 code to be stored, even in paper format. If provided on a paper authorization form, after the transaction is successfully processed, it is to be redacted on all stored documents.

When "Critical Confidential" information in paper form need no longer be stored for any operational or regulatory reason, it must be disposed of via cross-cut shredding or incineration. Any shredding bins that store "Critical Confidential" information prior to destruction will be kept locked at all times. Any digital information in the "Critical Confidential" category, whether on tape, CD/DVD, or located on a computer hard drive, will be completely erased and rendered unreadable by commercially reasonable methods. HBAGC has contracted with a third party for all storage of PANs, none will be stored by the company in digital form.) When feasible, non-critical "Confidential" information should be disposed of in the same manner.

Payment Processing System

HBAGC utilizes a web-based system provided via WebLink, by Authorize.Net, a PCI DSS Certified payment processing service provider, for all payment processing functions. All credit card and ACH transactions, whether authorized over the phone, in writing via mail, or online are transmitted, processed and stored via the Authorize.net system. Telephone and online transactions are directly entered into the system. Mailed transactions are entered into the system, and the paper authorization form is then stored in a secure locked cabinet or safe for only as long as required by business operational needs. In no circumstances are PANs stored electronically for any reason—secure storage is completely delegated to the Authorize.net system.

HBAGC employees have access to the Authorize.Net system for processing payments and reporting—but never have access to un-encrypted credit card or bank account numbers. Each User is granted system access permissions based on the minimum functionality required to perform job responsibilities.

During the course of performing their job responsibilities, HBAGC employees will have access to full credit card numbers, billing addresses, and CVV2 codes. HBAGC employees are expressly directed to enter this information directly into the WebLink system—and are never to record any PANs or CVV2s on paper, or to repeat or otherwise transmit this information to any third parties.

Access Controls

HBAGC employees will be granted access to sensitive company data and any archived authorizations or reports containing card data or other confidential customer information on a "need to know" basis. Access to payment processing systems and other company applications will also be granted on the basis of the minimum level required to perform assigned job responsibilities.

Key Access Control Provisions

- Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- A payment processing system Administrator will be responsible for issuing user accounts, provisioning user account permissions and processing limits, and monitoring system usage
- Access to the Authorize.net payment processing system, and all other connected systems, will be by individual username and password only. User accounts are not to be shared for any reason. Group User accounts and Generic User Accounts are prohibited.
- Payment processing, and all other connected system, passwords must be at least 8 alpha numeric characters and should not be written down.
- Passwords will expire every 90 days and must be unique over any 360 day period.
- User accounts will be locked after 5 consecutive failed logins.
- Any paper receipts, reports, or other documents containing cardholder data will be secured in a locked file drawer or safe, with access granted on a limited and documented basis. All documents containing cardholder data must be checked-out and checked-in by an authorized manager.
- A system Administrator will be notified of all employees leaving the company, or contractors whose services have been terminated, and immediately revoke access to all systems and storage facilities, including but not limited to the PaySimple Payment Processing system.

Network Security

HBAGC's network is designed, configured and maintained to deliver high performance and reliability to meet the needs of its members' while also providing access controls and necessary privileges. The intent of this policy is to protect our information assets, client data and reputation while providing secure and reliable services by implementing and managing technical safeguards on all critical systems and networks.

Key Access Control Provisions

- All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed. (If the account is to be disabled or deleted, the default password is changed first.)
- All unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled entirely before installation of a new system on the network.

Anti-Virus/Anti-Phishing

HBAGC has implemented Webroot® for the purpose of computer virus, worm and Trojan Horse prevention, detection and cleanup. In order to ensure the security of our computing environment, the following must be adhered to by all employees using HBAGC computers or systems:

- All computers accessing company systems, and/or utilizing the PaySimple payment processing system, must use the approved anti-virus/anti-phishing protection software and configuration.
- The virus/phishing protection software must not be disabled or bypassed.
- The settings and automatic update frequency for the virus/phishing protection software must not be altered in a manner that will reduce its effectiveness.
- Employees should NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.
- Employees should never download files from unknown or suspicious sources.
- Employees should never complete any forms accessed via links embedded in an email from an unknown, suspicious or untrustworthy source.

Acceptable Use

HBAGC is committed to protecting its employees, members, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. All computer related systems and equipment including but not limited to computer equipment, software, e-mail accounts, and web browsers are the property of HBAGC. All customer data obtained during the course of performing job responsibilities is the property of HBAGC. These systems and data are to be used for business purposes in serving the interests of the HBAGC, and our members in the course of normal operations. Effective security is a team effort involving the participation and support of every HBAGC employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee know these guidelines, and to conduct their activities accordingly.

Key Acceptable Use Policy Provisions

- Users should be aware that the data they create on the corporate systems remains the property of HBAGC. There is no expectation of privacy or guarantee of confidentiality of information stored on or accessed via any network, computer, or electronic device belonging to HBAGC.

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Authorize.net payment processing system passwords are changed every 90 days.

- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horse code, or other malware.

- Under no circumstances is an employee of HBAGC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing HBAGC-owned resources.

- The following activities are strictly prohibited, with no exceptions:

    - Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

    - Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

    - Circumventing user authentication or security of any host, network or account.

    - Providing information about, or lists of, HBAGC employees to parties outside HBAGC.

    - Providing information about or lists of HBAGC customers, including but not limited to PANs, and other sensitive customer information, to any external party or unauthorized internal party.

Vendor Management

All vendors that will have access to "Critical Confidential" information, including customer Credit Card numbers and Bank Account numbers, must be covered by a formal contract that includes the following guarantees:

- Service providers must comply with all PCI DSS requirements, and maintain and provide proof of PCI DSS certification as a service provider.

- Service providers must acknowledge responsibility for security of the cardholder data they possess, including but not limited to:

    - Protect cardholder data as specified by the PCI DSS, if processing or storing payment card data on behalf of HBAGC.

    - Report any known or suspect compromise of that data to the company as soon as possible.

    - Allow for audits by VISA/MasterCard/American Express/Discover or VISA/MasterCard/American Express/Discover-approved entities in the event of a cardholder data compromise.

    - Ensure continued security of cardholder data retained during and after contract terminations.

As part of the Vendor Management program, HBAGC will perform due diligence on each Vendor prior to signing any contract to confirm that the above guarantees have been adequately met.

HBAGC will maintain an up-to-date list of all service providers with access to "Critical Confidential" information. At a minimum this list will include the service provider's name, key contact information, they type of HBAGC confidential information to which the service provider has access, and the type of PCI responsibilities allocated to the vendor.

On at least a yearly basis, HBAGC will review the Service Provider List, and for all vendors that have access to "Critical Confidential" information to ensure that:

- PCI DSS compliance certification is up-to-date

- Other procedures in place to protect confidential information continue to adequately protect customers and are being properly executed

- Make any changes necessary to policies and procedures

Incident Response Plan

An Incident Response Plan is documented to provide a well-defined, organized approach for handling any security breach related to our customers' Personally Identifiable Information (PII). The Plan identifies and describes the roles and responsibilities of the {Company Name} Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

Security and Data Breach Definitions

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us, (for example, unauthorized use of a compromised User ID/Password to our payment processing system). Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

A data breach is defined as any unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a customer or employee of our organization.

Personally Identifiable Information (PII) is information that is, or can be, about or related to an identifiable individual. For our purposes, personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Social Security number
- Driver's license number or Identification Card number
- Medical or health information
- Financial account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account (including truncated account numbers).
- A User ID or Email Address and password, or User ID or Email Address and Security Question & Answer

This plan is designed to respond to a breach originating from HBAGC as well as to respond in the event that a breach of our customer data is reported to us by one of our Vendors.

Ranking Security & Data Breach Incidents

RED - These incidents may affect the integrity or confidentiality of data, which may result in direct loss of business and/or reputation, e.g. loss of large quantities of credit card account numbers.

YELLOW - These incidents typically affect small numbers of users and small amounts of data, or larger amounts of data with a very low probability that the data can or will be compromised (i.e. loss of encrypted data, or emailing a single PII record to the wrong person).

GREEN - These incidents may affect the confidentiality, integrity or availability of data however no actual breach has been confirmed. (i.e. unauthorized access to a system where it can be confirmed that no PII data was accessed or removed.)

Incident Response Team

Response to significant cyber incidents is guided by the company's Incident Response Team (IRT). Although first responders may be general IT staff or other company employees, the IRT provides overall response guidance. This team's first effort during an incident is to take control of the situation with the intent of mitigating potential damage to the company or its customers. It is the IRT's responsibility to:

- Manage the incident response process
- Defend against attacks and prevent further damage when an incident does occur
- Implement improvements that prevent attacks from reoccurring
- Report the outcome of any security incidents to the management team

The company has appointed a qualified IRT with current members listed in the following table.

IRT Member Title	Current IRT Member	IRT Member Contact Information
Executive Director	Dan Dressman	ddressman@cincybuilders.com
Finance Director	Beth Schramm	bschramm@cincybuilders.com
Operations Director	Karen Pfeiffer	kpfeiffer@cincybuilders.com

Incident Response Procedures

If any HBAGC employee becomes aware of a confirmed or potential breach, whether via direct knowledge or via a communication with a Vendor, an Incident will be deemed to have occurred, and the following procedure will be followed.

1. The incident is reported to the Incident Response Team (IRT) Leader.
2. The IRT Leader, in conjunction with the IRT and any other required personnel, identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach, of personal information about an individual.
3. If a breach is confirmed, the IRT ranks it RED, YELLOW, or GREEN and proceeds accordingly.
    a. GREEN incidents may be handled informally. At a minimum cause should be determined and future preventive measures implemented.
    b. YELLOW and RED incidents require further investigation, notification, and remediation, as described in the following steps.
4. Document all details of the incident.
    a. Determine if an unauthorized export or access to PII data has occurred.
    b. Determine where and how the breach occurred.
    c. Identify the source of compromise, and the timeframe involved.
    d. Identify all compromised or affected systems.
5. If the breach occurred at a third party vendor location, work with the vendor and review contract terms and determine next course of action.
6. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all systems and the number of individuals at risk.

7. Determine the type of personal information that is at risk, including but not limited to: Name, Address, Social Security Number, Account number, Cardholder name, Cardholder address, Medical and Health Information.
8. Take measures to contain and control the incident to prevent further unauthorized access to or use of PII.
9. Identify and contact the appropriate Data Owner affected by the breach. (Unless otherwise directed by law enforcement).
10. If credit cardholder data is involved, notify the Bankcard companies within 24 hours of compromise, unless otherwise instructed by law enforcement. (If the breach occurred at a Vendor location, work with the vendor to make this notification.)
11. If warranted, notify law enforcement of the breach.
12. Once the data breach has been contained, conduct a Lessons Learned session to determine how similar incidents may be prevented in the future.
13. Implement changes identified in Lessons Learned session.
14. IRT fully documents and closes incident.

Card Brand and Law Enforcement Contacts

Company	Contact Person/Department	Contact Information
Visa	Visa Incident Response	650-432-2978 usfraudcontrol@visa.com refer to Visa cisp what to do if compromised PDF
MasterCard	MasterCard Compromised Account Team	636-722-4100 compromised_account_team@mastercard.com
American Express	AMEX Security Breach Team	800-528-5200 Refer to AMEX DSOP service provider US document
Discover	Discover Network Incident Response Team	Merchants: 800-247-3083 Acquirers: 800-347-7052
Authorize.Net	Report security breech	
US Secret Service	Electronic Crimes Taskforce	305-863-5000
FBI	Report Internet Crime	www.ic3.gov/complaint
Ohio Attorney General	Report Fraud Crime	www.ohioattorneygeneral.gov/consumercomplaint 800-282-0515 Local: 614-466-4986