Square

Square Code of Business Conduct and Ethics

(Adopted On November 4, 2015; Effective As Of November 18, 2015; As Last Amended on October 23, 2019)

At Square, your work helps business owners everywhere start, run, and grow their businesses. This is exciting, inspiring work, and we expect that you approach it lawfully, honestly, ethically, and in the best interest of Square. This Code of Business Conduct and Ethics (**"Code"**) is your guide for such conduct, and the policies and procedures within show you how to uphold the Code in your day-to-day activities. For purposes of this Code, "we," "our," "Company," and "Square" refer to Square, Inc. and its subsidiaries.

The Board of Directors, in conjunction with the Audit and Risk Committee and the Nominating and Corporate Governance Committee, is ultimately responsible for administering this Code, and they have delegated day-to-day responsibility for administering and interpreting the Code to our General Counsel. The Nominating and Corporate Governance Committee is responsible for reviewing and monitoring compliance with the Code, including oversight over the establishment of procedures for the prompt internal reporting of violations of the Code. The Audit and Risk Committee will oversee the review of any complaints and submissions that have been brought to the Audit and Risk Committee by our General Counsel under the Code.

It is critical that all employees, officers, directors, agents, contractors, and any other individuals or party working on behalf of Square (all of whom we will refer to collectively as "you" and "Squares" throughout this Code) read, understand, and abide by the Code – so reference it frequently, talk to your lead, your Human Resources Business Partner (**"HRBP"**), the People Lead or the General Counsel about it, and ensure that you are following it with everything you do. These policies may not anticipate every situation, so it is important that you exercise good judgment in every decision you make and seek additional guidance when appropriate.

Beyond being responsible for following the Code, we must also hold each other accountable and report any violations. Individuals who violate the Code may be subject to disciplinary action, in accordance with applicable local law, up to and including termination of employment or the business relationship. If there is any conflict between this Code and applicable local law, you should comply with the most restrictive requirement.

Please take the time to review the information below and bring any questions to your lead, HRBP, the People Lead or the General Counsel at legal@squareup.com. Employees can find the name and contact information of their HRBP at go/myhrbp. Contingent workers and contractors can reach out to their agency-employer. Note: This Code sets forth a minimum standard; it does not reduce or limit the other legal and contractual obligations you may have to Square.

TABLE OF CONTENTS

Access Policy
Granting and Revoking Access
Access Systems
Handling and Classification of Data
Protection, Retention and Destruction
Software Development and Deployment
Production Systems and Network Security
Maintaining Security

AMENDMENTS, MODIFICATIONS AND WAIVERS

OUR RESPONSIBILITIES

Confidentiality and Communicating with External Parties

Protecting Square's Confidential Information is a critical responsibility for all individuals who perform work for Square, and violations of these obligations can have a serious impact on our business. While we are proud of significant milestones we have accomplished as a company, we need to protect Square's Confidential Information and be cautious in communicating any material, non-public information about the Company to anyone outside of the Company who is not bound by a confidentiality obligation to us (**"Third Parties"**). You should not share confidential information (or your opinions about such information) with people outside Square or people inside of Square who do not have a need to know this information. If you are uncertain about whether information is confidential, reach out to your lead and you can work together to ensure your actions comply with Square's policies.

Only our Chief Executive Officer, Chief Financial Officer, and Communications Lead (collectively, **"Spokespersons"**), and individuals explicitly authorized by a Spokesperson to speak on a particular topic or occasion (**"Delegates"**), as designated in the Company's External Communications Policy, may engage in discussions about the Company with Third Parties.

Unless you are a Spokesperson or Delegate, you are not authorized to speak with Third Parties on behalf of the Company, including the media, investors, or analysts, and should not give the impression that you are speaking on behalf of the Company in any communication. This includes any public speaking event and posts to online forums such as social media sites, blogs, chat rooms, and bulletin boards. This policy also applies to public comments about specific matters that relate to our businesses, as well as letters to the editor and endorsements of products or services. Please refer to our External Communications Policy

for more information.

Equal Employment Opportunity and Prohibition on Harassment

Square encourages a creative, culturally diverse, and supportive work environment. Employees and individuals performing services for Square are expected to create a respectful workplace culture that is free of harassment, intimidation, and unlawful bias and discrimination. Square is an equal opportunity employer and makes decisions based solely on individual merit and qualifications directly related to professional competence and objective business needs. Square strictly prohibits discrimination or harassment of any kind on the basis of race, color, religion, veteran status, national origin, ancestry, pregnancy status, sex, gender identity or expression, age, marital status, mental or physical disability, medical condition, sexual orientation or any other characteristics protected by law. Please review Square's Equal Employment Opportunity Policy and Policy Prohibiting Harassment for further information.

Drug and Alcohol Abuse Policy

Square prohibits individuals from being impaired under the influence of alcohol, as well as the unlawful use, possession, distribution, sale, or manufacture of any illegal drug or controlled substance on Square premises while conducting or performing Square business regardless of location; while operating or responsible for the operation, custody, or care of Square equipment or other property; or while responsible for the safety of Square employees, business partners, or customers

Square prohibits all individuals from working while impaired by the use of any legal drug whenever such impairment might endanger the safety of the individual or others, pose a risk of damage to Square property or equipment, or interfere with the individual's job performance or the efficient operation of Square business or equipment.
You are required to notify Square of any conviction under a criminal drug statute for a violation occurring in the workplace or during a Square-related activity or event, not later than five days after any such conviction. When required by federal law, Square will notify any federal agency with which it has a contract of any individual who has been convicted under a criminal drug statute for a violation occurring in the workplace. An individual who is convicted under a criminal drug statute for a violation occurring in the workplace will be deemed to have violated this policy.

If you suspect that you may have alcohol or drug problems, even in the early stages, you are

encouraged to voluntarily seek diagnosis and to follow through with the treatment as prescribed by qualified professionals. If you wish to voluntarily enter and participate in an approved alcohol or drug rehabilitation program, you are encouraged to contact your lead or your HRBP. Contingent workers and contractors should contact their agency-employer. Square will then determine whether it can provide an accommodation by providing a leave of absence for the time necessary to complete participation in the program. You should be aware that participation in a rehabilitation program will not necessarily shield you from disciplinary action for a violation of this policy, particularly if discipline is imposed for a violation occurring before you seek assistance.

Reporting and Speak-Up Policy

Trust forms the foundation of our business, and we operate on the basis of transparency, honesty, and trust with our customers, business partners, employees, and individuals performing services for Square. All are responsible for fostering a safe, respectful, productive environment, which means that you should report any concerns you have regarding a violation of Square's policies.

Consistent with our mission and core beliefs, we rely upon our officers, directors, employees, contractors, and others who do business with us to bring to light good faith concerns regarding Square's business practices, including: (1) reporting suspected legal violations by Square; (2) providing truthful information in connection with an inquiry or investigation by a court, an agency, law enforcement, or any other governmental body; and (3) identifying potential violations of the Code.

The integrity of our business practices and financial information is paramount. Our financial information guides the decisions of our management team and Board of Directors and is relied upon by our stockholders and the financial markets. For these reasons, we must maintain a workplace where individuals, when they reasonably believe that they are aware of questionable accounting, internal accounting controls, or other financial matters, or the reporting of fraudulent financial information (collectively, **"Fraudulent Activities"**), can raise these concerns free of any retaliation, discrimination, or harassment.

Reporting and Investigation

If you have a good faith concern regarding conduct that you believe to be a violation of law or Company policy (**"Violation"**), or a belief that any Violation or Fraudulent Activity has occurred or is occurring, you should:

- Discuss the situation with your lead or your HRBP or your agency-employer (if applicable); or
- If your lead is involved in the situation or you are uncomfortable speaking with your lead, contact your HRBP (and agency-employer if applicable) , the People Lead, General Counsel, or Chief Financial Officer (for international locations, you may also contact your Site Lead); or
- If you do not believe your concern is being adequately addressed, you are not comfortable speaking with one of the above-noted contacts, or you prefer to remain anonymous, you may report your concern via our reporting hotline at www.intouchwebsite.com/square (available to all individuals performing services for Square) or 855-339-2828 if you are in the U.S. or Canada, and 1-300-926-132 if you are in Australia, through which you may choose to identify yourself or remain anonymous. Concerns submitted through the reporting hotline that are financial or accounting related will be reviewed by a member of the Audit and Risk Committee and General Counsel or their delegates, as appropriate.

All reports will be taken seriously and will be promptly investigated appropriately. The specific action taken in any particular case depends on the nature and gravity of the conduct or circumstances reported and the results of the investigation. Where a Violation or Fraudulent Activity has been reported and confirmed, we will take corrective action proportionate to the seriousness of the offense. This action may include disciplinary action (in accordance with applicable local law) against the offending party, up to and including termination of employment or any other working relationship that the offending party may have with Square. Reasonable and necessary steps will also be taken to prevent any further Violation or Fraudulent Activity.

No Retaliation

We are committed to providing a work environment in which you feel free to raise any good faith concern, free of retaliation, discrimination, or harassment (**"Retaliation"**). Accordingly, Square will not tolerate any Retaliation against any individual who reports in good faith or participates in the investigation of any suspected Violation or Fraudulent Activity in accordance with this policy.

Nothing in this policy prevents you from reporting information to federal/national, state/provincial, or local law enforcement agencies when you have reasonable cause to believe that the violation of a law has occurred.

If you believe that you have been subject to Retaliation for having made a report in compliance with this policy or for having participated in any investigation relating to an alleged Violation or Fraudulent Activity, please immediately report any alleged Retaliation to your HRBP, the People Lead, General Counsel, or Chief Financial Officer. If, for any reason, you do not feel comfortable discussing the alleged Retaliation with these individuals, please report the alleged Retaliation through the reporting hotline at www.intouchwebsite.com/square (available to all individuals performing services for Square) or 855-339-2828 if you are in the U.S. or Canada and 1-300-926-132 if you are in Australia, through which you may choose to identify yourself or remain anonymous (note: you may still receive a response to your inquiry if you choose to remain anonymous by using a case number and password on our reporting hotline). Bringing any alleged Retaliation to our attention promptly enables us to honor our values and to promptly and appropriately investigate the reported Retaliation in accordance with the procedures outlined above. If a complaint of Retaliation is proven to be true, appropriate disciplinary action (in accordance with applicable local law) will be taken against the offending party, up to and including termination of employment or any other working relationship that the offending party may have with Square.

Cooperation and Confidentiality in Investigations

All individuals are expected to cooperate in good faith in any investigations, and provide complete and truthful information. All information disclosed during the course of the investigation will remain confidential, except as reasonably necessary to conduct the investigation, to allow the Company to take any remedial action and/or to comply with applicable law.

For any Violation or Fraudulent Activity not reported through an anonymous report, we will advise the reporting individual that the Violation or Fraudulent Activity has been addressed and, if we are able, of the specific resolution. However, due to confidentiality obligations, there may be times when we will not be able to provide the details regarding the corrective or disciplinary action that was taken.

Protected Communications

Nothing in Square's policies or in any agreement you enter into with Square restricts your rights (**"Protected Rights"**) to do any of the following:

- Engage in communications or actions protected by applicable law, such as certain

rights you may have to discuss wages and working conditions with other employees or personnel (with or without a union) under Section 7 of the National Labor Relations Act or under federal and state equal pay laws;

- File a charge with, or participate in an investigation conducted by, the Equal Employment Opportunity Commission, the National Labor Relations Board, the Occupational Safety and Health Administration, the Securities and Exchange Commission, or any other federal, state, or local governmental agency or commission (**"Government Agencies"**), and without notice to Square; or
- Receive an award for information provided to any Government Agencies.
- With respect to Confidential Information, you must not disclose more than is reasonably necessary to effect any Protected Rights you may have as identified above. For example, filing a charge with a Government Agency does not entitle you to divulge Confidential Information that is not relevant to the charge. "Confidential Information" is defined in the Confidential Information and Invention Assignment Agreement that you signed in connection with your work at Square, and it includes technical data, trade secrets, know-how, research, product or service ideas or plans, and other business information.

If you have any questions or concerns about whether an activity is allowed, please contact legal@squareup.com or reach out using our reporting hotline at www.intouchwebsite.com/square (available to all individuals performing services for Square) or 855-339-2828 if you are in the U.S. or Canada and 1-300-926-132 if you are in Australia, through which you may choose to identify yourself or remain anonymous (note: you may still receive a response to your inquiry if you choose to remain anonymous by using a case number and password on our reporting hotline).

Insider Trading Policy

You may not trade or enable others to trade Square stock or stock of another company, such as a customer, supplier, competitor, potential acquisition or alliance, while in possession of material non-public information about that company. Any questions as to whether information is material or has been adequately disclosed should be directed to the insider@ alias or the General Counsel. Additional information regarding insider trading can be found in our Insider Trading Policy.

Antitrust and Fair Dealing

Competing vigorously, yet lawfully, with competitors and establishing advantageous, but fair,

business relationships with customers and suppliers is a part of the foundation for long-term success. That being said, unlawful and unethical conduct, which may lead to short-term gains, would damage Square's reputation and long-term business prospects. Accordingly, you must comply with antitrust and competition laws and deal ethically and lawfully with our customers, suppliers, competitors, employees, and contractors in all business dealings on our behalf. You should not take unfair advantage of another person in business dealings on our behalf through the abuse of privileged or confidential information or through improper manipulation, concealment or misrepresentation of material facts, or any other unfair dealing practices.

Global Sanctions Policy

While performing official duties on behalf of Square, employees and contractors must adhere to the Global OFAC Policy ("GOP"). Under the GOP, employees and contractors are restricted from the following specific activities:

- Individuals performing services for Square cannot engage in activity that violates local sanctions law;
- While certain travel to comprehensively sanctioned countries and jurisdictions is permitted under current OFAC regulations, any business-related travel must be reviewed by the Sanctions Compliance Team, who are responsible for Square's enterprise-wide sanctions compliance program. Square employees and contractors must provide 14 days advance notice to the Sanctions Compliance Team, via email at us_sanctions@squareup.com, before such travel occurs. At no other time can Square employees and contractors conduct business for or on behalf of Square while in a country under comprehensive sanctions (i.e., Cuba, Iran, North Korea, Syria, Crimean Region of Ukraine).
- Individuals performing services for Square cannot access any Square issued or approved information technology hardware, software or any other Square system or program while in a comprehensively sanctioned country or jurisdiction.

If you have any questions or concerns, please contact the Sanctions Compliance Team at us_sanctions@squareup.com.

CONFLICTS OF INTEREST AND OUTSIDE ACTIVITIES

Conflicts of Interest Policy

You have a responsibility to avoid any situation that may create or appear to create a conflict between your personal interests and the interests of Square. Situations that commonly create conflicts of interest include (but are not limited to):

- Square business relationships with friends or relatives;
- Investing in a company that competes with Square's current or anticipated business; and
- Using Square's property, information, relationships, or your position for personal gain.

Many potential conflicts of interest are covered by our Outside Activities Policy (described below). You must disclose any actual or potential conflict of interest (or even the appearance of an actual or potential conflict of interest), including but not limited to the existence of any of the above situations, to your HRBP and Legal at legal@squareup.com. You must promptly take action to eliminate a conflict of interest if Square asks you to do so.

Gifts, Entertainment, and Favors

You may not accept gifts, entertainment, or other favors from a third party where doing so creates an appearance that such action was intended to influence a business decision, did influence a business decision, or created a reciprocal obligation. Business courtesies such as meals, tickets to sporting events, or similar entertainment are permitted if they are reasonable in cost and the purpose is to hold bona fide business discussions or to foster better business relations. Business courtesies exceeding $500 must be disclosed to your lead and your HRBP in advance.

You may only provide gifts, entertainment, or other favors to third parties on behalf of Square if they are of nominal value. Gifts, entertainment, or other favors may never be provided to government officials on behalf of Square without approval of Legal. Bribes and kickbacks – offering anything of value to obtain new business, retain existing business, expedite government actions, or secure any improper advantage – are strictly prohibited. More details on this are available in our Foreign Corrupt Practices Act and Anti-Corruption Policy and Guidelines.

Relationship Policy

Conflicts of interest not only arise based on your activities, but can also arise based on the activities of third parties in significant relationships (e.g., domestic partners, dating relationships, etc.). An actual or potential conflict of interest occurs when an individual is in a

position to influence a decision that may result in a personal gain for that individual as a result of business dealings with Square (e.g., a personal relationship with a subordinate employee or vendor). In addition, personal or romantic involvement with a competitor, supplier, subordinate employee of Square, or individual performing services for Square creates a potential or actual conflict of interest.

If you are involved in any of the types of relationships or situations described in this policy, you should immediately and fully disclose the relevant circumstances to your lead or your HRBP for guidance about whether a potential or actual conflict exists. When necessary, we will take appropriate action to manage the conflict based on the circumstances. In cases where there is an actual or potential conflict because of the relationship between employees or others engaged in business dealings with Square, even if there is no line of authority or reporting involved, Square may, in its sole discretion, make alternative reporting or decision-making arrangements, or may take appropriate action to resolve the conflict, to the extent permitted by applicable local law.

Employment of Relatives

Square may hire your relatives where there are no potential problems of supervision, morale, or potential conflicts of interest. Individuals who marry or become related will be permitted to continue to work at Square as long as there are no substantial conflicts. Reasonable accommodations will be made when possible in the event a conflict arises. For the purpose of this policy, a relative is any person who is related by blood or marriage, or whose relationship with the individual is similar to that of persons who are related by blood or marriage. You should immediately and fully disclose the relevant circumstances to your HRBP for guidance about whether a potential or actual conflict exists.

Outside Activities Policy

Outside activities must be pre-approved if they could interfere with your work performance or work schedule at Square, or if they could result in an actual or potential conflict of interest or the appearance of a conflict of interest. Outside activities include (but are not limited to) other employment, consulting, serving on a board or in another advisory capacity, and volunteer activities.

Even if the outside activity is approved, it must not interfere with your work performance or work schedule at Square, and it may not compete with Square's current or anticipated business. You may not use Square's property, facilities, equipment, systems, time, or brand

in connection with the outside activity, or disclose Square's confidential, proprietary, and trade secret information or otherwise violate the terms of your Confidential Information and Invention Assignment Agreement as outlined in your offer letter/employment agreement.

If you are interested in pursuing an outside activity, you may submit a Jira request at go/outsideactivities. Be sure to include:

- A full description of what you would be doing and, if applicable, the name of the organization;
- A description of any compensation you would receive (e.g., salary, equity, fees, commission, etc.);
- An estimate of the time commitment involved; and
- A discussion of how the work would relate to your role at Square. For instance, will this enhance skills you are using with the Company, or will it create beneficial exposure for Square? On the other hand, will it impact your work performance or work schedule at Square and detract from your participation in Company projects and activities?

Once your lead receives your request (and after asking any appropriate follow-up questions), he or she will bring it to your HRBP and Legal for consideration. We will collectively determine whether to approve the outside activity, and, depending on the request, we may escalate for discussion among the full leadership team. While every case is different, the factors we will consider in making these decisions may include:

- Is the proposed activity in any way competitive with Square's current or anticipated business? Would it entail the use of Company time, resources, or IP?
- Is the activity and the commitment it entails consistent with the expectations for the work or services you perform at Square?
- Will the proposed activity advance Square's interests in any way?
- Is this a for-profit undertaking or does it involve open-source or volunteer work?
- How is the individual doing at Square overall?

Corporate Opportunities

Individuals performing services for Square owe a duty to the Company to advance its legitimate business interests when the
opportunity to do so arises. You may not take the following actions, unless such actions are approved or ratified in accordance with Square's conflict of interest approval procedures:

- Diverting to yourself or to others any opportunities that are discovered through the use of Square's property or information, or as a result of your position with the Company, unless such opportunity has first been presented to, and rejected in writing by, the General Counsel;
- Using the Company's property or information or your position for improper personal gain; and
- Competing with Square.

Political Affiliations

If you contribute time or money to any political activity, you must comply with all laws, regulations, and Square policies regarding gifts to, and entertainment of, governmental officials. You may not use Square's stationery, the Square name or logo, work titles with Square, or subordinates to express personal political opinions, promote candidates, or seek political contributions.

In addition, if you become involved with a political group, you must make it clear that your activities are being conducted purely in a personal capacity and not on behalf of or in connection with the Company.

Reporting Concerns

If you become aware of any actual or potential conflict of interest, bribe/kickback, or other ethical concern at Square, immediately report your concern to your lead, your HRBP, the People Lead, or the General Counsel, even if you are not sure whether the conduct violates this or any other Square policy. Contingent workers and contractors can reach out to their agency-employer. Square does not permit retaliation of any kind for reports of misconduct made in good faith or cooperation in any investigation of such reports. Please refer to the Reporting and Speak-Up Policy (described below) for additional information.

INFORMATION & TECHNOLOGY POLICIES

Computer Equipment Use Policy

We may issue you computer equipment (**"Gear"**) to foster collaboration, communication, security, and enhanced productivity. We expect you to use Gear for:

1. Communications and work product on Square's systems, such as email, word processing, spreadsheets, and other related documents, video and audio

communications that are either live or pre-recorded, and web-based collaboration;
2. Use of software for productivity, such as graphic, audio, or video editing programs, word processing, spreadsheet, or other related productivity software, software engineering platforms, and accounting or finance related programs;
3. Access to networked services, such as servers, network devices, firewalls, and software programs related to the function of Square's business; and
4. Use of social media services such as Twitter, Facebook, Instagram, and other external public services for business purposes such as marketing, research, customer service, external communication, or other related public relations activities.

Personal use, which is defined as limited, occasional, or incidental access to electronic media (sending or receiving) for nonbusiness purposes is also okay. However, knowingly transmitting, retrieving, or storing any communication that is discriminatory or harassing, obscene, sexually explicit or pornographic, defamatory or threatening, in violation of any license governing the use of software, in violation of copyright law, or any purpose that is insecure, illegal or contrary to Square's policy or business interests (**"Bad Stuff"**) is prohibited. If you engage in Bad Stuff, you will be subject to disciplinary action (in accordance with applicable local law), up to and including termination of employment.

Please note that Bad Stuff does not include use of Gear for conduct protected by Section 7 of the National Labor Relations Act, such as lawful discussions about wages, hours or working conditions, nor does it include use of Gear for reporting potential violations of the law to a government agency or other law enforcement organization.

You should not assume that any communications on Square systems are completely private. All communications on Square systems may be subjected to capture or monitoring (in accordance with applicable local law), whether intentional or unintentional, by IT standards and procedures. Any personal data stored on Square's devices, networks, or servers remains Square property, to the extent permitted by applicable local law.

You are expected to operate your Gear in a reasonably safe manner. You should make every reasonable attempt to prevent your Gear from becoming damaged or a security vulnerability for Square.

Lost or stolen Gear should be reported to the IT team immediately. Instructions will be provided to help with recovery of the issued Gear, or instructions for replacement Gear will

be offered.

Damaged Gear should be returned to the IT team for repair or replacement. You can find additional policies at go/IT.

Personally Identifiable Information Policy

Personally Identifiable Information (**"PII"**) is extremely sensitive, and if lost or improperly disclosed, it could be extremely damaging to Square, our customers, and their customers. Certain roles at Square require access to PII, and individuals who access PII must adhere to our data policy (available at go/datapolicy) and the security policy set forth below.

Breaches of either of these policies may result in termination and/or prosecution.

Definitions

- "PII" means anything classified as Secret Data, PCI data, or Basic PII in our data policy.
- "Bulk PII" means greater than 1,000 elements of PII, where a single row may contain multiple elements.
- "Non-Bulk PII" means 1,000 or fewer elements of PII, where a single row may contain multiple elements.
- "Client machine" means a host machine provisioned for analytics that contains PII.
- "Access" means to access, copy, export, move, manipulate, transform, analyze, or otherwise use PII located in a Square database, system, or client machine, without making the contents of PII visible to human eyes.
- "View" means to use PII in such a way that its contents are visible to human eyes.
- "Row" means a line returned in response to a database query.
- "Element" means a part of a row.

PII and Bulk PII Access Policy

Individuals may access PII only when, and to the extent, necessary to perform their jobs.

Individuals cannot export PII from its authorized location (including a Square database, system, or client machine) or make it accessible to anyone who does not have authorized access to that location, unless and only to the extent they have obtained advance written permission from the Information Security and Privacy Counsel teams to do so. Absent such

advance written permission, individuals may export statistics on PII but not the PII itself. If individuals do not know whether certain information is PII, they must obtain from the Information Security and Privacy Counsel teams either (a) advance written permission to export that information or (b) confirmation that the information is not PII before exporting it.

Individuals cannot view Bulk PII unless, and only to the extent, it is necessary to perform their jobs and they have obtained advance written permission from the Information Security and Privacy Counsel teams to do so.

Individuals may view Non-Bulk PII only when, and to the extent, necessary to perform their jobs, with advance permission from the Information Security and Privacy Counsel teams to do so.

All actions taken by individuals relating to PII may be logged and audited. This includes, but is not limited to, accesses and views of PII on Square databases, systems, and client machines.

Individuals are responsible for ensuring and maintaining the security of the client machines and tools they use.

INFORMATION SECURITY POLICY

Roles and Responsibilities

We all have a shared duty to protect Square's intellectual property, data and other business assets. We take our intellectual property, data, business systems, and network security very seriously. Good security, working practices, and procedures for Square property, in all its forms, are critical in protecting the data and intellectual property development that fuels Square's growth, the livelihood of our employees, and our collective investment in Square. Square's files, networks, software, internet access, internet browser programs, email, voice mail, and other business equipment and resources are provided for business use, and they are the exclusive property of Square. Misuse of such property is not tolerated.

The Information Security team is responsible for providing overall guidance and direction in information security at Square. We work with other teams and management to develop and implement:

- Detailed policies, standards, and procedures appropriate to Square's needs and responsibilities;

- Day-to-day monitoring and audit programs; and
- An incident response and escalation program.

If you need assistance, you can reach us at infosec@squareup.com.

Access Policy

We must ensure Square deploys logical and physical access controls that provide appropriate protection for the data and systems they cover. The Information Security team is responsible for developing effective access control procedures. Where reasonable and appropriate, these procedures must:

- Grant access to sensitive data and systems on a “need to know” basis and in accordance with our data policy (go/datapolicy);
- Grant only the least privileges required for the task at hand;
- Include a formal, documented process for granting and revoking access; and
- Ensure that requirements for two-factor authentication, password complexity, and other technical controls are appropriate to business risks and satisfy all regulatory requirements.

Square employees, contractors, and other personnel must not attempt to gain unauthorized access to data and systems, or to circumvent access control systems. All access to Square resources must be in compliance with this policy and the data policy.

Granting and Revoking Access

Access to systems and resources is granted based on your role. The IT team is responsible for creating initial accounts for users; any exceptions to the standard access roles must be approved by the Information Security team.

If an individual requires a password reset, the user’s identity must be appropriately verified before any change is made.

Square reserves the right to modify or revoke an individual’s access at any time. Individuals who experience a change in employment status (e.g., termination or position change) must have their access rights promptly reviewed and, if necessary, modified or revoked. Upon termination of employment, the IT team will disable an individual’s access and retains the right to delete any Square-owned information from any personal mobile devices that were connected to Square’s network. The Information Security team is responsible for conducting

a periodic audit to ensure that access rights are appropriate.

Access to Systems

All employees and contractors must be issued a unique user ID, as shared-access accounts are prohibited. All accounts with access to sensitive user data must have strong passwords as described in the Password Policy. Systems with access to sensitive data must lock out users after 15 minutes of inactivity, whether through automatic logoff or password-protected screensaver mechanism.

All administrative access to systems must have audit trails that link the actions taken to the specific individuals who performed them. The Information Security team is responsible for reviewing these logs on a periodic basis to ensure that the controls in place are effective.

Handling and Classification of Data

Square processes and stores many kinds of data, including some that are extremely sensitive. We will use the following terms in classifying data, as well as the more nuanced classifications described in the data policy at go/datapolicy:

- Public: Data that is generally accessible and not otherwise restricted. A merchant's name, for example, is Public data.
- Sensitive: Any Confidential or Highly Confidential (Secret and PCI) data.
- Confidential: Data that should not be shared with the general public, but which may be shared with that data's owner. This includes, for example, user email addresses or phone numbers.
- Highly Confidential (Secret and PCI data): Data whose unauthorized disclosure or modification might cause serious harm to users, to Square, or to Square's partners. This includes social security numbers, payment card data and bank account numbers, for example.

The Head of Information Security will maintain an inventory of the data types stored on Square systems, along with their classification in this scheme. See also Data Policy.

Protection, Retention, and Destruction

In general, Square will retain the minimum amount of Sensitive data required for business, legal, and regulatory purposes. Sensitive data that does not need to be retained will be purged or deleted in a secure fashion. The following data elements must never be stored in

any form after processing:

- Magnetic stripe data;
- CVC2/CVV2/CID/CAV2; and
- PIN/PIN Block

Confidential data must be stored using commercially reasonable security standards and practices as advised by Information Security. Highly Confidential data must be stored in encrypted form or tokenized according to Information Security standards, or as otherwise authorized by Information Security. If Confidential or Highly Confidential data is transmitted over a public network or stored on a third-party service, it must be protected according to Information Security standards.

The Head of Information Security is responsible for developing and maintaining day-to-day procedures that meet these requirements and are appropriate to Square's business needs and regulatory requirements.

Software Development and Deployment

We are committed to the security and stability of the service Square provides to customers. To that end, the Head of Information Security is responsible for maintaining and enforcing standards regarding secure application development and deployment. These standards must specify, at a minimum:

- Appropriate use of cryptography, as specified in the Cryptography and Encryption policy;
- Code review requirements for all Sensitive code deployed in a production context;
- Testing and validation against standards such as PCI DSS §6.3 and the OWASP Top Ten list;
- Regression and acceptance testing as necessary;
- Appropriate documentation of changes and their impact;
- Appropriate sign-off or approval as needed; and
- Back-out procedures as necessary.

Production Systems and Network Security

Network Configuration Standards

The Head of Information Security is responsible for maintaining formal standards for network equipment, including firewalls and routers, that apply to all networks storing or processing

Highly Classified information. These standards must specify:

- Appropriate documentation of all firewall rules and their business justification;
- Periodic review of rules and configuration; and
- Other, specific requirements as defined in the PCI DSS.

System Configuration Standards

The Head of Information Security is responsible for ensuring that appropriate system configuration and hardening standards exist for all systems storing or processing Highly Classified information. These standards must be based on and consistent with best-practice documents from groups such as NIST and SANS, and they must meet all regulatory requirements, including those specified in PCI DSS §2.2.

Vulnerability Management

The Head of Information Security is responsible for maintaining a vulnerability and patch management program. This program will require that, where feasible:

- All critical security patches be applied within 30 days;
- Anti-virus software be active and up to date on all systems commonly affected by malware; and
- All systems be periodically assessed for vulnerabilities.

Maintaining Security

Hiring

Prior to hiring, all individuals are screened (in accordance with applicable local law), which may include background checks, credit checks, reference checks, and other forms of verification. In each case, the hiring manager, in conjunction with the People and Counsel teams, is responsible for determining the appropriate screening. Contractors or personnel engaged to perform work for Square may be screened by their agency-employer or vendor. Hiring managers must also ensure that employees, contractors, and other personnel have the knowledge and training necessary to be able to carry out their information security responsibilities.

Testing

Square will perform both internal and external penetration tests of all systems containing or

processing Highly Classified data. These tests must meet, at a minimum, the requirements of PCI §11 and must be performed at least quarterly, as well as after any significant changes. The Head of Information Security is responsible for ensuring these tests are performed and reviewing the results of third-party testing and for ensuring the timely remediation of any problems found.

Logging

To the extent possible and reasonable, all Square systems must be configured to store log and audit trail information. These logs must include all relevant details of the event and must be stored for at least one year. The Head of Information Security is responsible for defining procedures that ensure these logs are audited in a timely manner and for conducting periodic tests to ensure that these logs are sufficient for forensic analysis.

Incident Response

The Head of Information Security and the Head of Business Continuity Management are responsible for ensuring that the Company on-call process meets all requirements for incident response plans specified in industry standards such as the PCI DSS (§12.9). This plan must be tested at least annually.

Risk Assessment

At least once a year, the Head of Information Security will work with other members of Square's management to conduct a formal, documented risk assessment. This risk assessment will identify:

- Threats to Square's business, customers, and systems;
- Relative likelihood and impact of these threats;
- Overall control objectives to mitigate identified risks; and
- Technical and procedural controls to meet these objectives.

Security Awareness

The Head of Information Security is responsible for conducting an ongoing security awareness and training programs. This program is intended to ensure that individuals are aware of their responsibilities with respect to security and that they have the knowledge and training necessary to be able to carry out these responsibilities. All individuals must attend security awareness training upon hire and at least annually.

Partners

The Head of Information Security and privacy vetting must take place for any third party partner who is proposed to access or process sensitive information on behalf of Square. The Head of Information Security and Privacy Counsel will maintain a due diligence process for vetting third party providers. This process must meet at least the requirements specified in PCI DSS §12.8.

AMENDMENTS, MODIFICATIONS, AND WAIVERS

We are committed to continuously reviewing and updating our policies, and therefore reserve the right to amend this Code at any time, for any reason, subject to applicable law. Any amendment or modification of the Code must be approved by our Board of Directors and promptly disclosed in accordance with applicable laws and regulations.

Any waiver of any provision of the Code for an executive officer or director of the Company must be approved by our Board of Directors, or a committee authorized by our Board of Directors, and promptly disclosed pursuant to applicable laws and regulations. Any waiver of any provision of the Code for any other employees, officers, agents, contractors, individuals performing services for Square, and parties working on behalf of the Company or any of its direct and indirect subsidiaries must be approved by the General Counsel.