Important information. Please read and save for your records.

This agreement and disclosure (“Agreement”) refer to Merck Employees Federal Credit Union’s digital banking services, which include: online banking, mobile banking, our automated Telephone Teller, internet and intranet Web Sites, our Home Banking feature and our Online Bill Payer system (additional sign-up required). With Digital Banking Services (“Digital Banking”), you'll be able to perform virtually all your credit union transactions from your home, office, or almost anywhere there is cell phone reception or a touchtone phone.

By using any of our Digital Banking services, you agree to the terms of this Agreement & Disclosure Statement. Joint account holders and other persons that are authorized to use your Digital Banking services are also bound by the terms and conditions contained in this Agreement & Disclosure Statement. The User ID and Password used for Digital Banking services is the signature of the owner of the account and identifies an individual who is authorized to conduct transactions from the account and validates the directions given just as the actual signature and other proof of identity validate the directions of the account owner.

In this agreement, the words "you" and "your" mean each person who has signed any Digital Banking service request, or who uses your Digital Banking services with your consent. "We," "us" and "our" mean the Merck Employees Federal Credit Union, MEFCU. "Account" means each of your accounts which you access through our Digital Banking platforms. You can enroll in any of our Digital Banking services at any time.

We may offer additional Digital Banking transaction services from time to time and/or change or charge fees. If we do, all subsequent transactions initiated by you or performed by us will be subject to this agreement. Notice of changes in service or charges will be forwarded in writing to your last known address at least twenty-one (21) days prior to their effective date.

Joint account holders and other persons authorized to use your Digital Banking services are also bound by the terms and conditions contained in this Agreement & Disclosure.

For questions related to our Digital Banking services, please contact us at 732-484-4811.

Your Responsibilities:

You will select a password or PIN for Digital Banking. We recommend following the current best practices for password/PIN complexity to ensure your safety. You must use this password each time you log into online or mobile banking. You will also be required to set up an additional layer of security. This will be either multi-factor authentication using a phone number to receive a call or text, an authenticator application downloaded onto your mobile phone or other device, or email to receive the code (though not the safest option). For telephone teller, you will select a four (4) to fifteen (15) digit numerical PIN. This PIN is different from the PIN used for your ATM/Debit Card.

Joint Owner Usage. You may authorize the joint owners of your account to utilize Digital Banking services by disclosing your password or PIN to them. Be advised that your password or PIN grants access to all share and loan sub-accounts of your primary account number and you agree that you are responsible for all transactions initiated by your password or PIN.

Safeguarding your password and PIN. Your password and PIN are confidential. The use of the password or PIN with our Digital Banking services is a security method by which the Credit Union is helping you maintain the security of your account(s). Therefore, you agree to protect your password and PIN. Take all reasonable precautions to ensure that no one else learns your password and PIN. Do not reveal your password and PIN to anyone who is not allowed to access your account. We will not be responsible for losses which occur because of transactions performed by someone you provided access to your Digital Banking account(s).

Wrongful Use. If someone uses your password or PIN without your consent, you agree to provide us with a written sworn statement and will help us investigate and prosecute the wrongful use. The statement must be written on our form and completely filled in. We do not have to credit you for those losses before you give us

this statement. Merck Employees Federal Credit Union also reserves the right to charge a depositor for reasonable costs and expenses incurred in conducting an error investigation when it is determined that no error has occurred.

Ending Authorized Use. If someone else is allowed to use your password or PIN and you want to end that person's use, change your password or PIN through the Digital Banking system impacted or contact the credit union.

Password/PIN. To protect the privacy of your account, you will have the only record of the password and PIN you have chosen. If you lose it or forget it, you will have to select a new password or PIN. Transmission of confidential business and sensitive personal information is at user's sole risk. You agree to indemnify, hold harmless, and defend Merck Employees Federal Credit Union from and against any and all claims actions, suits, judgements and expenses (including court costs and reasonable fees of attorneys, accountants and expert witnesses) at user's sole expense, arising from user's failure to abide by these restrictions or use of the Digital Banking services.

Termination. The Credit Union may cancel this Agreement and your use of any of the Digital Banking services at any time without notice. We can change the terms or conditions of this Agreement and Disclosure Statement without telling you, unless it is required by law. You agree and acknowledge upon termination of services to immediately cease using the services.

Charges/Fees. You agree to pay and hereby authorize the Credit Union to charge your Credit Union account(s) for all transactions which you initiate through use of any Digital Banking service.

Limitations on the Use of Any Digital Banking Service. You will be denied the use of Digital Banking for payments or account transfers if (a) you do not have adequate funds available in your accounts or available overdraft protection, or (b) you do not enter the correct PIN. There is a limit on the number of denials permitted, and you will be denied access to the service if you exceed these limits.

Payments and other transactions conducted on a business day are posted to your Credit Union accounts within two (2) business days. Payments and other transactions conducted on a Saturday, Sunday or Federal Holiday will be posted to your account within two business days.

The following uses of Digital Banking services are strictly prohibited:

Unauthorized communication of any charge or credit card information belonging to any other person or entity.

Unauthorized communication of any information concerning any password, other online access number, code, identification or any other proprietary information belonging to any other person or entity.

Use of Digital Banking services to copy or to distribute or transmit copies of copyrighted materials belonging to any other person or entity is permitted only to the extent that the owner has provided express permission to the user permitting such activity.

In violation of any telecommunication, postal, or other local laws or regulations of the user's country of origin or of the U. S. or in furtherance or in the commission of any crime or other unlawful or improper purpose.

Communicating any obscene or defamatory information including, but not limited to, bulletin boards or in conjunction with e-mail.

Merck Employees Federal Credit Union reserves the right to monitor and review transmissions online and in storage, and to remove or reject any material which we, in our sole discretion, believe may be unlawful or objectionable, without prior notice to user.

You may use Digital Banking services to:

Make withdrawals from your Checking (share draft), special accounts and regular share accounts (except IRA). A check payable to the account holder will be mailed from the Credit Union on the following business day to the address currently on file for you.

Transfer funds between your Checking (share draft) and regular share accounts or transfer to loan accounts.

Obtain account balances.

Obtain information about the last dividend paid to an account.

Obtain tax information including total interest paid and dividends earned from the previous year.

Obtain information about drafts/checks cleared, deposits and withdrawals within current history.

Change your username, password or PIN.

Make Cross Account Transfers.

Complete an online Loan application.

. View eStatements, tax forms and notices (additional sign up required)

Loss or Theft/Liability. Tell us at once if you believe your password or PIN has been lost or stolen. You can also update your online banking and mobile banking passwords yourself using the online service. Remember that it is possible to lose all the money in your accounts (plus your maximum line of credit, when available).

If you do not tell us within two (2) business days after you learn of the loss or theft of your password or PIN, and we have proof that we could have stopped someone from using your Digital Banking services without your permission if you had told us, you could lose as much as $500.

Also, if your statement shows transactions you did not make, tell us at once. If you do not tell us within sixty (60) days after the statement was provided to you, you may not get back any money you lost after the sixty (60) days if we can prove that we could have stopped someone from taking the money had you told us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we will extend the time period.

Correcting Errors.

In case of errors, if you think your statement is wrong, if you have questions about your transactions or, if you need more information about a transaction listed on the statement, telephone us at (732) 594-3317 or email us at memberservices@merckefcu.com immediately. We must hear from you no later than sixty (60) days after we send the FIRST statement on which the problem or error appears. Please give us your name and describe the error or transaction in question and explain as clearly as possible why you believe it is an error or why you need more information. Tell us the dollar amount of the suspected error. If you tell us orally, we may require that you send and we receive your complaint or question in writing within ten (10) business days.

We will tell you the results of our investigation within ten (10) business days after we hear from you and will correct any error promptly. We will notify you if additional time is necessary as it may take up to forty-five (45) days to investigate your complaint or question. If so, your account will be credited within ten (10) business days for the amount you think is in error. If we ask you to put your complaint or question in writing and we do not receive it within ten (10) business days, we may not adjust your account. If we decide that there was no error, we will send you a written explanation within three (3) business days after we finish our investigation. You may ask for copies of the documents that we used in our investigation. A fee may be charged for these copy requests.

Business Days

Our business days and hours are 8 am - 4:00 pm, Monday through Friday. Holidays are not included.

Disclosure of Account Information

Merck Employees Federal Credit Union will not provide copies of documents or reports used in our investigations when to do so would violate the privacy rights of our other depositors. We will disclose information to third parties about your accounts or the transactions you make:

Where it is necessary for completing transactions

In order to verify the existence and condition of your account for a third party, such as a credit bureau or merchant.

In order to comply with a government agency or court orders.

If you give us your permission.

If it involves a claim against us on an item deposited to or drawn against your account.

If it is allowed under state or federal privacy laws.

Limit on Liability

Unless otherwise required by law, we will not be responsible for any losses or damages from the use of the services described in this Agreement, including direct, indirect, special or consequential losses or damages. In any case, we shall only be liable for the actual proven damages if the failure to make the transactions:

Is not intentional.

Is the result of mistakes made in good faith.

Should have been prevented by our usual practices.

Any cause of action concerning Digital Banking services under this Agreement must be commenced within one year after such cause of action has occurred.

Periodic Statements

You will get a monthly account statement unless there are no transfers in a particular month.

Identity Verification Program

NOTE: Message & Data rates may apply. To cancel, text "STOP" to the number that texted the most recent text. In case of questions please contact Member Services at 732-594-3317.

Additional Digital Banking Terms & Conditions

Merck Employees Federal Credit Union offers mobile access to authenticate a user over SMS. Enrollment requires identification of the user's banking relationship as well as providing a mobile phone number. The mobile phone number's verification is done by the user receiving an SMS message with a verification code which they will have to enter on the website. This program will be on-going. Message & Data rates may apply. Users will be allowed to opt out of this program at any time.

To Stop the program: To stop the messages from coming to your phone, you can opt out of the program via SMS. Just send a text that says "STOP" to the number sending the alerts. You'll receive a one-time opt-out confirmation text message. After that, you will not receive any future messages.

Terms & Conditions: By participating in Verification Alerts, you are agreeing to the terms and conditions presented here.

Our participating carriers include (but are not limited to) AT&T, T-Mobile®, Verizon Wireless.

Privacy and User Information. You acknowledge that in connection with your use of Digital Banking, Merck Employees FCU and its affiliates and service providers, including Alkami and its affiliates, may receive names, domain names, addresses, passwords, telephone and device numbers, the content of messages, data files, data about your usage of the service (such as session length, number of transactions and geolocation), and other data and information provided by you or from other sources in connection with Digital Banking or the Software (collectively "User Information").

Merck Employees FCU and its affiliates and service providers will maintain reasonable safeguards to protect the information from unauthorized disclosure or use, but reserve the right to use and disclose this information as reasonably necessary to deliver Digital Banking, perform analytics to improve the service, and as otherwise permitted by law, including compliance with court orders or lawful instructions from a government agency, to protect the personal safety of subscribers or the public, to defend claims, and as otherwise authorized by you.

Merck Employees FCU and its affiliates and service providers also reserve the right to monitor use of Digital Banking and the Software for purposes of verifying compliance with the law, these terms and conditions and any applicable license, but disclaim any obligation to monitor, filter, or edit any content.

Restrictions on Use. You agree not to use Digital Banking or the Software in or for any illegal, fraudulent, unauthorized or improper manner or purpose and will only be used in compliance with all applicable laws, rules and regulations, including all applicable state, federal, and international Internet, data, telecommunications, telemarketing, "spam," and import/export laws and regulations, including the U.S. Export Administration Regulations.

Without limiting the foregoing, you agree that you will not use Digital Banking or the Software to transmit or disseminate: (i) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom you do not otherwise have a legal right to send such material; (ii) material that infringes or violates any third party's intellectual property rights, rights of publicity, privacy, or confidentiality, or the rights or legal obligations of any wireless service provider or any of its clients or subscribers; (iii) material or data, that is illegal, or material or data, as determined by Merck Employees FCU (in its sole discretion), that is harassing, coercive, defamatory, libelous, abusive, threatening, obscene, or otherwise objectionable, materials that are harmful to minors or excessive in quantity, or materials the transmission of which could diminish or harm the reputation of Merck Employees FCU or any third-party service provider involved in the provision of Digital Banking; (iv) material or data that is alcoholic beverage-related (e.g., beer, wine, or liquor), tobacco-related (e.g., cigarettes, cigars, pipes, chewing tobacco), guns or weapons-related (e.g., firearms, bullets), illegal drugs-related (e.g., marijuana, cocaine), pornographic-related (e.g., adult themes, sexual content), crime-related (e.g., organized crime, notorious characters), violence-related (e.g., violent games), death-related (e.g., funeral homes, mortuaries), hate-related (e.g. racist organizations), gambling-related (e.g., casinos, lotteries), specifically mentions any wireless carrier or copies or parodies the products or services of any wireless carrier; (v) viruses, Trojan horses, worms, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or personal information; (vi) any material or information that is false, misleading, or inaccurate; (vii) any material that would expose Merck Employees FCU, any third-party service provider involved in providing Digital Banking, or any other third party to liability; or (viii) any signal or impulse that could cause electrical, magnetic, optical, or other technical harm to the equipment or facilities of Merck Employees Federal Credit Union or any third party.

You agree that you will not attempt to: (a) access any software or services for which your use has not been authorized; or (b) use or attempt to use a third party's account; or (c) interfere in any manner with the provision of Digital Banking or the Software, the security of Digital Banking or the Software, or other customers of Digital Banking or the Software; or (d) otherwise abuse Digital Banking or the Software.

Use of Google Maps: You agree to abide by the Google terms and conditions of use found at http://maps.google.com/help/terms_maps.html and the Google Legal Notices found at http://www.maps.google.com/help/legal notices_maps.html, or other URLs as may be updated by Google.

Biometric Authentication for Digital Banking. Biometric Authentication (fingerprint or facial recognition) is an optional sign-in method for Merck Employees FCU Mobile Banking that is currently available for most mobile devices. Biometrics are stored on your device only and Merck Employees FCU never sees or stores your biometric information. You acknowledge that by enabling biometric authentication, you will allow anyone who has a biometric authentication method stored on your device access to your personal and payment account information within Merck Employees FCU Mobile Banking. Merck Employees FCU reserves the right to suspend or disable this feature at any time.

If your device doesn't recognize your biometric authentication method, you can sign in using your password. You can enable or disable biometric authentication anytime from within the Merck Employees FCU Mobile Banking application.

The following supplemental Terms of Use ("Supplement") applies to the card controls feature ("Card Controls") within the Mobile Banking mobile application ("Mobile Banking App"), notwithstanding anything in the Agreement to the contrary. The Supplement only applies to Card Controls. If Card Controls are not available to you, then this Supplement does not apply. To the extent there is any conflict between the terms of the Agreement and this Supplement with respect to Card Controls, then the terms in this Supplement shall apply. 1. The Card Controls feature is only available for debit and credit cards issued by Merck Employees FCU that you register within the Mobile Banking App. 2. The Card Controls alerts and controls you set through use of the Mobile Banking App may continue to apply, even if you delete the Mobile Banking App or remove it from your mobile device. Please contact Merck Employees FCU to discontinue the alerts and controls. 3. Certain Card Control functionality within the Mobile Banking App may not be available for all transactions. Controls and alerts based on the location of the mobile device where the Mobile Banking App is installed or the location of the merchant where the card is being attempted for use may not apply appropriately to card-not-present transactions or transactions where the actual location of the merchant differs from the merchant's registered address. 4. Card Controls may enable access to Merck Employees FCU and third parties' services and web sites, including GPS locator websites, such as Google's. Use of such services may require Internet access and that you accept additional terms and conditions applicable thereto. 5. To the extent this Mobile Banking App allows you to access third party services, Merck Employees FCU, and those third parties, as applicable, reserve the right to change, suspend, remove, or disable access to any of those services at any time without notice. In no event will we be liable for the removal of or disabling of access to any such services. We may also impose limits on the use of or access to certain services, in any case and without notice or liability. 6. THE MOBILE BANKING APP, THE SERVICES AND RELATED DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON- INFRINGEMENT. IN PARTICULAR, WE DO NOT GUARANTEE CONTINUOUS, UNINTERRUPTED OR SECURE ACCESS TO ANY PART OF OUR SERVICE, AND OPERATION OF THE MOBILE BANKING APP OR THE SERVICES MAY BE INTERFERED WITH BY NUMEROUS FACTORS OUTSIDE OF OUR CONTROL. SOME STATES DO NOT ALLOW THE DISCLAIMER OF CERTAIN IMPLIED WARRANTIES, SO THE FOREGOING DISCLAIMERS MAY NOT APPLY TO YOU TO THE EXTENT THEY ARE PROHIBITED BY STATE LAW. 7. Limitation of Liability. YOU ACKNOWLEDGE AND AGREE THAT FROM TIME TO TIME, THE MOBILE BANKING APP AND THE SERVICES MAY BE DELAYED, INTERRUPTED OR DISRUPTED FOR AN INDETERMINATE AMOUNT OF TIME DUE TO CIRCUMSTANCES BEYOND OUR REASONABLE CONTROL, INCLUDING BUT NOT LIMITED TO ANY INTERRUPTION, DISRUPTION OR FAILURE IN THE PROVISION OF THE SERVICES, WHETHER CAUSED BY STRIKES, POWER FAILURES, EQUIPMENT MALFUNCTIONS, INTERNET DISRUPTION OR OTHER REASONS. IN NO EVENT SHALL WE OR OUR AFFILIATES OR LICENSORS OR CONTRACTORS OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY CLAIM ARISING FROM OR RELATED TO THE SERVICES THAT IS CAUSED BY OR ARISES OUT OF ANY SUCH DELAY, INTERRUPTION, DISRUPTION OR SIMILAR FAILURE. IN NO EVENT SHALL WE

OR OUR AFFILIATES OR LICENSORS OR CONTRACTORS OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, OR LOSS OF GOODWILL OR LOST PROFITS (EVEN IF ADVISED OF THE POSSIBILITY THEREOF) ARISING IN ANY WAY OUT OF THE INSTALLATION, USE, OR MAINTENANCE OF THE MOBILE BANKING APP, OR THE SERVICES, OR THE WEBSITES THROUGH WHICH THE MOBILE BANKING APP OR THE SERVICE OFFERED, EVEN IF SUCH DAMAGES WERE REASONABLY FORESEEABLE AND NOTICE WAS GIVEN REGARDING THEM. IN NO EVENT SHALL WE OR OUR AFFILIATES OR LICENSORS OR CONTRACTORS OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE BE LIABLE FOR ANY CLAIM, ARISING FROM OR RELATED TO THE MOBILE BANKING APP, THE SERVICES OR THE WEBSITE THROUGH WHICH THE APP OR THE SERVICES IS OFFERED, THAT YOU DO NOT STATE IN WRITING IN A COMPLAINT FILED IN A COURT OR ARBITRATION PROCEEDING WITHIN TWO (2) YEARS OF THE DATE THAT THE EVENT GIVING RISE TO THE CLAIM OCCURRED. THESE LIMITATIONS WILL APPLY TO ALL CAUSES OF ACTION, WHETHER ARISING FROM BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL THEORY. OUR AGGREGATE LIABILITY, AND THE AGGREGATE LIABILITY OF OUR AFFILIATES AND LICENSORS AND CONTRACTORS AND THE EMPLOYEES AND CONTRACTORS OF EACH OF THESE, TO YOU AND ANY THIRD PARTY FOR ANY AND ALL CLAIMS OR OBLIGATIONS RELATING TO THIS AGREEMENT SHALL BE LIMITED TO DIRECT OUT OF POCKET DAMAGES UP TO A MAXIMUM OF $500 (FIVE HUNDRED DOLLARS). SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. 8. Unless our account agreement with you states otherwise, this Agreement shall be governed by and construed in accordance with the laws of the State in which you reside, without regard to its conflicts of laws provisions. To the extent that the terms of this Agreement conflict with applicable state or federal law, such state or federal law shall replace such conflicting terms only to the extent required by law. Unless expressly stated otherwise, all other terms of this Agreement shall remain in full force and effect. Alerts Additional Terms. The following Alerts terms and conditions ("Alerts Terms of Use") only apply to the Alerts feature (as defined below). If Alerts are not available to you, then this Alerts Terms of Use does not apply. To the extent there is any conflict between the terms of the Agreement and this Alerts Terms of Use with respect to Alerts, then the terms in this Alerts Terms of Use shall apply. Alerts. Your enrollment in Merck Employees FCU Online Banking and/or Mobile Banking (the "Service") includes enrollment to receive transaction alerts and notifications ("Alerts"). Alerts are electronic notices from us that contain transactional information about your Merck Employees FCU account(s). Alerts are provided within the following categories: • Mandatory Alerts provide you with important account notifications, such as information about changes to your Online Banking password, PIN, or login information. You do not have the option to suppress these Mandatory Alerts. • Account Alerts provide you with notification of important account activities or when certain changes are made to your Service accounts. These Alerts are automatically activated for you. Although you may suppress these Account Alerts, we strongly recommend that you do not do so because they provide important information related to your Service accounts. • Additional Alerts must be activated by you to be enabled. Account Alerts and Additional Alerts must be managed and/or added online through the Service. You cannot maintain all Alerts through your mobile device. We may add new Alerts from time to time, or cancel old Alerts. We usually notify you when we cancel Alerts, but are not obligated to do so. Merck Employees FCU reserves the right to terminate its Alerts service at any time without prior notice to you.

Methods of Delivery. We may provide Alerts through one or more channels ("EndPoints"): (a) a mobile device, by text message; (b) a mobile device, by push notification; (c) an email account, by an e-mail message; or (d) your Merck Employees FCU Digital Banking message in-box, by an e-mail message. You agree to receive Alerts through these EndPoints, and it is your responsibility to determine that each of the service providers for the EndPoints described in (a) through (c) above supports the email, push notification, and text message Alerts provided through the Alerts service. Please be advised that text or data charges or rates may be imposed by your EndPoint service provider.

Alert frequency varies by account and preferences. You agree to provide us a valid mobile phone number or email address so that we may send you Alerts. If your email address or your mobile device's number changes,

you are responsible for informing us of that change. Your Alerts will be updated to reflect the changes that you communicate to us with regard to your primary and secondary email addresses or mobile device number.

Alerts via Text Message. To stop Alerts via text message, text "STOP" to 39872 at anytime. Alerts sent to your primary email address will be unaffected by this action. To restore Alerts on your mobile phone, just visit the Alerts tab in Merck Employees FCU Online Banking and click the box next to your mobile number for the Alerts you'd like to receive again. For help with SMS text alerts, text “HELP” to 39872. In case of questions please contact customer service at 732-594-3317. Our participating carriers include (but are not limited to) AT&T, SprintPCS, T-Mobile®, U.S. Cellular®, Verizon Wireless, MetroPCS.

Limitations. Merck Employees FCU provides Alerts as a convenience to you for information purposes only. An Alert does not constitute a bank record for the deposit or credit account to which it pertains. We strive to provide Alerts in a timely manner with accurate information. However, you acknowledge and agree that your receipt of any Alerts may be delayed or prevented by factor(s) affecting your mobile phone service provider, internet service provider(s) and other factors outside Merck Employees FCU’s control. We neither guarantee the delivery nor the accuracy of the contents of each Alert. You agree to not hold Merck Employees FCU, its directors, officers, employees, agents and service providers liable for losses or damages, including attorneys' fees, that may arise, directly or indirectly, in whole or in part, from (a) a non-delivery, delayed delivery, or the misdirected delivery of an Alert; (b) inaccurate or incomplete content in an Alert; or (c) your reliance on or use of the information provided in an Alert for any purpose.

Alert Information. As Alerts delivered via SMS, email and push notifications are not encrypted, we will never include your passcode or full account number. You acknowledge and agree that Alerts may not be encrypted and may include your name and some information about your accounts, and anyone with access to your Alerts will be able to view the contents of these messages. Privacy and User Information – Data Analytics. You acknowledge that in connection with your use of Digital Banking, Merck Employees FCU and its affiliates and service providers, including Alkami. and its affiliates, may receive data about your usage of the service (such as session length, number of transactions and geolocation), and other data and information provided by you or from other sources in connection with Digital Banking or the Software. Merck Employees FCU and its affiliates and service providers will maintain reasonable safeguards to protect the information from unauthorized disclosure or use, but reserve the right to use and disclose this information as reasonably necessary to deliver Digital Banking, perform analytics to improve the service, and as otherwise permitted by law, including compliance with court orders or lawful instructions from a government agency, to protect the personal safety of subscribers or the public, to defend claims, and as otherwise authorized by you.

Card Management Additional Terms The card management feature is offered by Merck Employees FCU (referred to herein as “CardHub”, “us”, “we” or “our”) for use by Merck Employees FCU cardholders. Merck Employees FCU’s card management feature is intended to allow You to initiate certain payment card related activities for Your enrolled Merck Employees FCU card(s) via the card management feature. Those activities may include the ability to but not limited to: • Register the card • Activate and deactivate the card • Set control preferences for card usage including location, transaction, and merchant types, spend limits, and card on/off (“Controls”) • Set alert preferences for card usage including location, transaction, and merchant types, spend limits, and declined purchases (“Alerts”) • View transaction history including cleansed and enriched merchant information (e.g., merchant name, address, and contact information) • Report Your card as lost or stolen • Review Your spending by merchant type and/or by month • View a list of merchants storing Your card information for recurring or card-on-file payments The card management feature may enable access to Merck Employees FCU and third parties’ services and web sites, including GPS locator websites, such as Google. Use of such services may require internet access and that You accept additional terms and conditions applicable thereto, including, with respect to Google maps, those terms and conditions of use found at http://maps.google.com/help/terms_maps. Html and the Google Legal Notices found at https://www.google.com/help/legalnotices_maps/, or such other URLs as may be updated by Google. To the extent the card management feature allows You to access third party services, Merck Employees FCU and those third parties, as applicable, reserve the right to change, suspend, remove, limit, or disable access to any of those services at any time without notice and without liability to You. You agree to allow us to communicate with You

via push notification, SMS and/or email, with respect to the activities performed via the card management feature. Data fees may be imposed by Your mobile provider for the transmission and receipt of messages and Alerts. Merck Employees FCU reserves the right to send administrative and service notifications via emails and/or SMS messages to the email address and/or phone number provided upon enrollment in Merck Employees FCU's card management feature. Availability/Interruption. You acknowledge that the actual time between occurrence of an event ("Event") triggering a selected Control or Alert and the time the notification of such event is sent to Your mobile device ("Notification") is dependent on a number of factors including, without limitation, Your wireless service and coverage within the area in which You are located at that time. You acknowledge that Notifications of Events may be delayed, experience delivery failures, or face other transmission problems. Similarly, selection of Controls and Alerts (collectively, "Commands") are likewise affected by the same or similar factors and problems could arise with use of Commands. Notifications of Events may not be available to be sent to Your mobile device in all areas. If You registered to receive Notifications to Your mobile device, the card management feature is available when You have Your mobile device within the operating range of a wireless carrier with an appropriate signal for data services. The card management feature is subject to transmission limitations and service interruptions. Merck Employees FCU does not guarantee that the card management feature (or any portion thereof) will be available at all times or in all areas. You acknowledge and agree that certain functionality with the card management feature may not be available for all transactions. Commands based upon the location of the mobile device where the card management feature is installed or the location of the merchant where the card is being attempted for use may not apply appropriately to card-not-present transactions or transactions where the location of the actual location of the merchant differs from the merchant's registered address. You acknowledge and agree that neither Merck Employees FCU nor its third-party services providers (including the developer of the technology enabling the Notifications) are responsible for performance degradation, interruption or delays due to conditions outside of its control. You acknowledge that neither Merck Employees FCU nor its third-party service providers shall be liable to You if You are unable to receive Notifications on Your mobile device in Your intended area. Merck Employees FCU, for itself and its third-party service providers, disclaims all liability for: any delays, mis-delivery, loss, or failure in the delivery of any Notification; any form of active or passive filtering.