Answers to Common Questions about Custodial Services

This document answers the most common questions that employers have when selecting Optum Bank (the "Bank"), Member FDIC, as the preferred custodian for their employees' health savings accounts (HSAs). We are happy to answer any additional questions you may have and look forward to working with you to ensure that your employees' HSA enrollment process is easy and rewarding and that they can make the most of their HSAs.

Is the Bank a trustee or a custodian of HSA funds?

The Bank is a custodian of individual employee HSAs, not a trustee or a plan administrator. As such, the Bank holds and ensures the safekeeping of HSA funds, maintains accurate records, responds to account holder instructions and other responsibilities. The Bank does not have any discretionary authority over the funds in an account and has no fiduciary obligations.

In providing HSA custodial services, the Bank enters into a deposit and custodial agreement with each individual employee. The deposit and custodial agreement establishes a contractual banking relationship directly between the bank and each employee and is supervised by the state of Utah and the FDIC.
The Bank complies with all federal and state laws and regulations applicable to financial institutions and HSAs, most notably: the Right to Financial Privacy Act, the USA Patriot Act, the Gramm-Leach-Bliley Act (GLBA), and the Internal Revenue Code. The Bank's policies and procedures, including the contracting and enrollment process, are designed to fulfill the Bank's legal obligations to each individual account holder.

Are HSAs employee welfare benefit plans subject to ERISA?

HSAs are not considered employee welfare benefit plans under the Employee Retirement Income Security Act of 1974 (ERISA). However, certain actions by employers can trigger ERISA applicability. If an employer triggers ERISA, HSAs change from voluntary employee individual bank accounts to employee welfare benefit plans and the HSAs become group health plans under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Consolidated Omnibus Budget Reconciliation Act (COBRA) as well. The consequences of triggering ERISA impact both the employer and the Bank and may include extensive reporting and bookkeeping, plan documents for HSAs, HIPAA application, fiduciary responsibilities, COBRA requirements and exposure to class action ERISA litigation.

Department of Labor guidance explains what employers may or may not do with regard to HSAs to avoid triggering ERISA. In sum, employer involvement with HSAs must be very limited. Employers are permitted to open HSAs for their employees and deposit funds only because the employees will still have exclusive responsibility for spending and controlling funds. Employers may also limit the HSA providers it allows to market products in the workplace or select a single provider. However, employers may not:

- Limit the ability of eligible individuals to move their funds to another HSA
- Impose impermissible conditions on using HSA funds
- Make or influence the investment decisions for funds contributed to an HSA
- Define the HSAs as an employee welfare benefit plan established or maintained by the employer
- Receive any payment or compensation in connection with an HSA
- Contribute to an HSA by means of a salary reduction to which the employee does not consent
- Limit the number of HSA providers and receive discounts on other products

Is the Bank a vendor / service provider to the employer or health plan?

In providing HSA custodial services, the Bank enters into a deposit and custodial agreement with each individual employee. The agreement establishes a contractual banking relationship directly between the bank and each account holder and is supervised by the state of Utah and the FDIC. As a result, the Bank is a service provider to each individual account holder. To ensure that the Bank complies with all applicable statutes and regulations, including compliance with customer privacy and data and security standards, the Bank is audited annually by the state of Utah and the FDIC.

Answers to Common Questions about Custodial Services

Since the HSAs offered by the Bank are not employee welfare benefit plans or components of such plans, they are not subject to ERISA or HIPAA. While an employer may act as an agent on behalf of its employees to open and contribute to an HSA, to avoid the unnecessary and costly applicability of ERISA to employers and the Bank, employer involvement must be limited and any perception or implication that the HSA is maintained or controlled by the employer must be avoided. Consequently, the Bank is unable to agree with any requirement that the Bank enter into a vendor relationship with an employer or assume any liability or obligation that could be perceived as the employer maintaining and controlling the HSA with the Bank.

Why is the Bank's contracting process different from other banks that offer HSA custodial services?

The Bank is different from many other banks offering HSAs because Optum Bank's primary product is custodial services for HSAs. In contrast, other bank may require employers to enter into a services agreement so that other services beyond HSAs can be added. These services might include lockboxes, wellness services, prescription drug discounts, health care plan administration, or other services that would require them to comply with HIPAA.

Since the Bank only provides HSA custodial services and because those services are provided to account holders and not the employer, the Bank does not need a services agreement with an employer. In fact, for most employers that select the Bank as their custodian of choice, an agreement with an employer is unnecessary. The only circumstances that require an agreement at all is when an employer wants to open HSAs or make contributions on behalf of their employees. In those limited circumstances, the Bank requires the employer to sign an HSA Enrollment and Contribution Agreement which is much narrower in scope than a general services agreement.

Why does the Bank require an HSA Enrollment and Contribution Agreement?

Typically, the Bank interacts with each individual account holder to obtain all of the information and documentation needed by the Bank to open an HSA in accordance with applicable banking laws and regulations. The Department of Labor has issued guidance that states that an employer may act as an employee's agent to open an HSA and to make contributions without implicating ERISA.

The primary purpose of the HSA Enrollment and Contribution Agreement is to allow the Bank to rely on the agency relationship between the employer and its employees to obtain the information and documentation needed by the Bank to open an HSA. When an employer chooses to open accounts for its employees, the Bank must rely on the employer instead of the account holder to meet the legal requirements necessary to open an account with a financial institution.

To help ensure that there are no ERISA or HIPAA implications that attach to the employer opening accounts and making contributions, the Bank carefully limits the scope of its legal agreement with the employer to merely ensure the employer is authorized to act as an agent for its employees and that the requirements of the USA Patriot Act and GLBA are satisfied.

Is a Business Associate Agreement needed in connection with the Bank's HSA custodial service?

HIPAA imposes strict privacy and security regulations on "covered entities" (including health providers, health plans, and health care clearinghouses) and their business associates. Covered entities and business associates are required to have business associate agreements (BAAs) with service providers where Protected Health Information (PHI) or Electronic PHI (EPHI) is involved. The Bank does not need to sign a BAA because it is not a covered entity or business associate. It is not a covered entity because it is not a health provider, health plan or health care clearinghouse and it is not a business associate because it does not send or receive the type of information that would classify it as a business associate.

Furthermore, the Bank is not subject to HIPAA because section 1179 of HIPAA excludes financial institutions when they are engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a

payment for, or related to, health plan premiums or health care, where such payment is made by any means including a credit, debit, or other payment card, an account check, or electronic funds transfer for itself or on behalf of a financial institution.

What information or data is passed back and forth between the Bank and an employer?

Employers that choose to open HSAs for employees are merely acting as agents for their employees in this process. As their agent, an employer must send employee information to the Bank on behalf of their employees which includes names and social security numbers. The Bank opens the HSAs and sends a file back to the employer as an "account number file" with account open dates, account numbers, and account status notes. The account number file (including name, social, and account data) is considered non-public personal information (NPPI) under GLBA. Once received, the employer can begin to make contributions to the HSAs and with each contribution file, will send contribution instructions to the Bank.

In the HSA Enrollment and Contribution Agreement, why does the Bank require that a non-bank employer be subject to GLBA?

The Bank, as a financial institution, is subject to and compliant with the requirements of GLBA and is audited for compliance by the state of Utah and FDIC. GLBA governs how financial institutions deal with the private information of individuals and regulates the collection and disclosure of private financial information and NPPI. Under GLBA, financial institutions must, among other requirements, implement data security programs to protect the NPPI of its account holders. The Bank's GLBA obligations are to the account holder, not the employer, since the NPPI is owned by the account holder.

Employers that open HSAs for employees receive an "account number file" from the Bank that contains account names, social security numbers, open dates, account numbers, and account status notes. Even though some of the data contained in the account number file originated with the employer, the employee data sent to the Bank is owned by the employee, not the employer. Furthermore, the employee data is not NPPI while it is in the possession of the employer, it is confidential information governed by the agency relationship between the employer and the employee.

Once the Bank receives information for the purpose of opening an HSA, either from an employee or an employer, under GLBA that information is now owned by the Bank and the employee/account holder. When the Bank sends a file back to the employer with account open dates, account numbers, and account status notes, that file now contains NPPI under GLBA. Since the Bank is sharing NPPI with a non-affiliated third party of the Bank, the recipient of the NPPI is required to comply with GLBA. Therefore, in order to comply with the provisions of GLBA, before the Bank shares NPPI with an employer it ensures in its HSA Enrollment and Confidentiality Agreement that each employer that receives NPPI from the Bank will comply with GLBA.

Does the Bank sign data security agreements with employers?

The Bank, as a financial institution, is subject to and compliant with the requirements of GLBA and is audited for compliance by the state of Utah and FDIC. GLBA governs how financial institutions deal with the private information of individuals and regulates the collection and disclosure of private financial information and NPPI.

Under GLBA, financial institutions must, among other requirements, implement data security programs to protect the NPPI of its account holders. The Bank's GLBA obligations are to the account holder, not the employer, since the NPPI is owned by the account holder.

The only information that employers send to the Bank is employee enrollment data and contribution instructions. That data is confidential information, but it is not NPPI. Once it is received by the Bank and used to open an account, the data becomes NPPI owned by a financial institution and the account holder, and the Bank is obligated to the account holder to protect it under GLBA. To protect that data under GLBA, an employer that receives an

Answers to Common Questions about Custodial Services

account number file from the Bank must agree to comply with GLBA in the HSA Enrollment and Contribution Agreement. This is not a mutual obligation because the Bank's obligations under GLBA are not to the employer; they are to the account holder. All of the Bank's obligations to the account holder are governed by the deposit and custodial agreement.

Are there advantages to opening an HSA in Utah?

According to the IRS, qualified medical expenses may be paid or reimbursed from an HSA starting on the date the account is actually "established" under state trust law. Many states require that an account be opened *and funded* in order to be established. This means that if an HSA is opened on January 1st, but not funded until the first paycheck is received or even six months later, then the account holder may not use the account to reimburse medical expenses incurred before the account was funded.

The Bank is a Utah state chartered financial institution. Utah trust law has closed the funding gap, allowing an account to be established before funding. This is administratively easier and also ensures that HSA holders get the maximum tax benefit with regard to the reimbursement of qualified medical expenses.