Envista
credit union

Rev. 11/17

# FACTS

## WHAT DOES ENVISTA CREDIT UNION DO WITH YOUR PERSONAL INFORMATION?

| | |
|---|---|
| **Why?** | Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do. |
| **What?** | The types of personal information we collect and share depend on the product or service you have with us. This information can include:<br>▪ Social Security number and account balances<br>▪ account transactions and credit history<br>▪ employment information and mortgage rates and payments<br><br>When you are *no longer* our member, we continue to share your information as described in this notice. |
| **How?** | All financial companies need to share members' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their members' personal information; the reasons Envista Credit Union chooses to share; and whether you can limit this sharing. |

| Reasons we can share your personal information | Does Envista Credit Union share? | Can you limit this sharing? |
|---|---|---|
| **For our everyday business purposes –** such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or to report to credit bureaus | Yes | No |
| **For our marketing purposes –** to offer our products and services to you | Yes | No |
| **For joint marketing with other financial companies** | Yes | No |
| **For our affiliates' everyday business purposes –** information about your transactions and experiences | No | We don't share |
| **For our affiliates' everyday business purposes –** information about your creditworthiness | No | We don't share |
| **For nonaffiliates to market to you** | No | We don't share |

| | |
|---|---|
| **Questions?** | Call toll-free 1-877-968-7528 or go to www.envistacu.com |

## What we do

| | |
|---|---|
| **How does Envista Credit Union protect my personal information?** | To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. |
| **How does Envista Credit Union collect my personal information?** | We collect your personal information, for example, when you<br>▪ open an account or provide account information<br>▪ apply for financing or give us your contact information<br>▪ show us your driver's license<br><br>We also collect your personal information from others, such as credit bureaus, affiliates, or other companies. |
| **Why can't I limit all sharing?** | Federal law gives you the right to limit only<br>▪ sharing for affiliates' everyday business purposes – information about your creditworthiness<br>▪ affiliates from using your information to market to you<br>▪ sharing for nonaffiliates to market to you<br><br>State law and individual companies may give you additional rights to limit sharing. |

## Definitions

| | |
|---|---|
| **Affiliates** | Companies related by common ownership or control. They can be financial and nonfinancial companies.<br>▪ *Envista Credit Union has no affiliates*. |
| **Nonaffiliates** | Companies not related by common ownership or control. They can be financial and nonfinancial companies.<br>▪ *Envista Credit Union does not share with our nonaffiliates so they can market to you.* |
| **Joint Marketing** | A formal agreement between nonaffiliated financial companies that together market financial products or services to you.<br>▪ *Our joint marketing partners include insurance companies.* |

## Other important information

**Application Data Management Methodology:**

Within the Visa infrastructure, data is securely stored and transmitted using standard industry practices that adhere to PCI-DSS security standards. Specifically, Visa adheres to the following principles:
• Data in transit is encrypted.
– For transmission of sensitive data within internal networks, the channel is encrypted.
– For external transmissions, the data and channel are both encrypted.
• Sensitive data at rest is encrypted. Data at rest (stored in the database) is protected through the following controls:
– Production systems are protected using a Visa zone security architecture that ensures bank data at rest is in restricted zones that are segmented from other zones, and that Visa corporate networks are segmented by firewalls and not accessible from the Internet.
– Firewall restrictions include: IP, application, and data type.1/14/20
– Procedures are in place for strict logical access to data; access to production data is on an individual and by-request basis, restricted to promote separation of duties, and inclusive of annual access certifications.
– IDS/IPS are in place with the zone architecture to prevent common application attacks.
• PI are collected, received, used, processed, stored and/or disclosed in accordance with the requirements defined by the Key Controls, the European General Data Protection Regulation (GDPR), California Consumer Protection Act (CCPA), the Gramm Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standards (PCI-DSS), the Personal Information Policy and Records, and Information Management Policy.
• Visa engages a qualified security assessor (QSA) annually to validate Visa's compliance with PCI-DSS.
In order to provide services to cardholders, we collect and store the following information on our secure infrastructure:
• Mobile account information
– Username
– Password
• Device information
– Manufacturer
– Model
– Operating system
– Unique device identifiers
– IP addresses
• Cardholder information
– First Name
– Last Name
– Email Addresses
– Phone Numbers
• Card details
– Card number1/14/20
– Card Expiration Date
– Billing Address
– Card Nickname
– CVV2 (collected for validation purposes but not stored)
• Why do we store the above-referenced data?
– For security purposes, we store device information and monitor activity.
– For analytical and reporting purposes, we store information about mobile application usage and participation in card services.
– For customer service and troubleshooting purposes, we store detailed information about system events.
• No sensitive information is stored on the mobile device. However, the following may be securely stored on the device:
– Payment tokens may be stored in a secure cryptography protected white box.
– Long-lived user tokens used for fingerprint authentication.
• In cases where data must be passed to external systems/parties to support a service, cardholders must opt-in to the service via the app.