Card Program Privacy Notice

Effective date: 30 September 2025. Last updated: 22 September 2026..

1. About this notice

This notice explains how Connect Fintech Services, Inc., doing business as Connect Financial ("Connect Financial", "we", "us"), handles personal data in the payment card programs we manage.

It applies to:

- Applicants for a card
- Cardholders and authorized users
- Directors, officers, beneficial owners and authorized representatives of businesses that apply for or hold cards
- Individuals who contact us about a card program

It does not apply to visitors to our website or business contacts outside a card program. Our privacy policy for these purposes can be found at https://connect.financial/company/privacy.

Read this notice with:

- The Cardholder Agreement for your card.
- The privacy notice of the Program Client that offers your card.

2. Who is involved in your card program

A card program involves several parties. Each has a different role.

Party	Who they are	What they do
Issuing Bank	The regulated bank that issues your card. It is named on your card and in your Cardholder Agreement.	Holds the card account. Ultimately responsible for identity verification, anti-money laundering, sanctions and fraud controls.
Program Client	The business that offers the card to you, usually through its own app or platform.	Manages its relationship with you. Usually your first point of contact.
Connect Financial	The program manager. Manages the card program for the Issuing Bank and the Program Client.	Licensed program operator. Runs onboarding and executes compliance controls on the Issuing Bank's behalf. Runs card operations and support services.
Card Network	The payment network whose brand appears on your card.	Routes and settles transactions. Manages tokens for digital wallets.
Service Providers	Companies that provide services to Connect Financial.	Process data on our instructions only.

3. Our role and responsibility for your data

Connect Financial is a "controller" when we decide why and how your data is used. For other activities we act on the instructions of the Issuing Bank or the Program Client. In those cases we are a "processor" or "service provider".

The Issuing Bank is ultimately responsible for identity verification, anti-money laundering, sanctions and fraud controls on your card. We carry out these controls on the Issuing Bank's behalf, under the Issuing Bank's program requirements and oversight.

Activity	Connect Financial's role	Notes
Identity verification, customer due diligence and business verification (KYC and KYB)	Processor for the Issuing Bank	The Issuing Bank is responsible. Connect Financial executes on its behalf. See Section 3.1.
Anti-money laundering monitoring, sanctions screening and regulatory reporting	Processor for the Issuing Bank	The Issuing Bank is responsible. Connect Financial executes on its behalf. Applies to every program.
Card and transaction fraud prevention	Processor for the Issuing Bank.	The Issuing Bank is responsible. Connect Financial executes on its behalf.
Security of Connect Financial's systems	Controller	Connect Financial is responsible for protecting the systems it operates.
Card issuance, account operations and transaction processing	Processor for the Issuing Bank	Performed under our agreement with the Issuing Bank.
Program services delivered through the Program Client's app (card controls, alerts, statements)	Processor for the Program Client	Performed under our agreement with the Program Client.
Disputes and chargebacks	Processor for the Issuing Bank	Handled under Card Network rules.
Cardholder support	Processor for the Program Client	Provided as a white-label service. Support staff may present under the Program Client's or Connect Financial's name

3.1 How identity verification works

The Issuing Bank sets the verification and due diligence requirements for every card program. Connect Financial applies them on the Issuing Bank's behalf. Who collects your information depends on the program.

Model A: Connect Financial performs verification

- You submit information and documents through the Program Client's app or a Connect Financial interface.
- Connect Financial, or a Service Provider acting for Connect Financial, verifies your identity, screens you against sanctions and watch lists, and assesses risk, on behalf of the Issuing Bank.
- Connect Financial decides whether the Issuing Bank's requirements are met, under the Issuing Bank's oversight.
- Connect Financial shares the outcome with the Program Client and the Issuing Bank as needed to operate the program.

Model B: The Program Client performs verification under an approved exception

- The Program Client has been approved by Connect Financial to collect and verify your information itself.
- The Program Client must meet the Issuing Bank's verification requirements.

- The Program Client shares your verification data and results with Connect Financial.
- Connect Financial reviews and monitors the results on behalf of the Issuing Bank. Connect Financial may ask for more information or documents.
- Connect Financial continues to carry out anti-money laundering, sanctions and fraud controls on the program for the Issuing Bank.
- The Program Client is responsible for its own collection of your data. Its privacy notice explains this.

Your Program Client can tell you which model applies to your card.

4. Personal data we handle

Category	Examples
Identity	Full name, date of birth, nationality, occupation, source of funds and gender, only where required by law or the Issuing Bank.
Government identifiers	Tax identification number, national identity number, passport or driver's license number
Verification	Images of identity documents, proof of address, a selfie or short video used for identity matching (see Section 7), verification results
Contact	Residential address, email address, phone number
Business (business programs)	Business name, registration details, ownership structure. Names, dates of birth, addresses and identification of directors, officers, beneficial owners and authorized representatives.
Card and account	Card token, last four digits, expiry date, card status, balance, limits and card controls. Connect Financial does not store full card numbers (see Section 12).
Transaction	Amount, date, merchant name, category and location, authorization outcome, disputes, funding and payouts
Screening and risk	Sanctions and watch list results, politically exposed person status, adverse media, fraud and risk scores, investigation records
Device and technical	IP address, device identifiers, operating system, browser, app version, approximate location from IP address, login times.
Communications	Support requests, emails, complaint records, call recordings.

Some of this data is sensitive under data protection law, for example biometric data, government identifiers and precise location. We use it only for the purposes in this notice.

Politically exposed person screening may reveal information about a person's public or political role. We process this only to meet legal obligations.

5. Where we get your data

- From you, through the Program Client's app or a Connect Financial interface
- From the Program Client, including under Model B verification
- From the Issuing Bank
- From the Card Network and digital wallet providers, for example when you add your card to a wallet
- From merchants, through the Card Network, as part of transaction data

- From identity verification, fraud prevention and screening Service Providers
- From public sources such as sanctions lists, government and company registers, public records and news media
- From your device, when you use an app or interface that Connect Financial provides

6. How we use your data and our legal basis

Some laws require us to state a legal basis for each use. The table sets these out. Where Connect Financial acts for the Issuing Bank, the legal basis is the Issuing Bank's, including its legal obligations as a regulated bank.

Purpose	Legal basis
Verify identity and carry out due diligence, at onboarding and during the relationship	Legal obligation (anti-money laundering and counter terrorist financing laws). Legitimate interests (managing program risk).
Screen against sanctions, watch lists and politically exposed person lists	Legal obligation
Monitor transactions for financial crime and report suspicious activity to authorities	Legal obligation
Detect and prevent fraud and protect accounts	Legitimate interests. Legal obligation where it applies.
Issue and manage cards, process transactions, and move funds	Performance of the Cardholder Agreement
Send alerts, statements, receipts and service messages	Performance of the Cardholder Agreement. Legal obligation.
Handle support requests, disputes and complaints	Performance of the Cardholder Agreement. Legal obligation. Legitimate interests.
Match your selfie to your identity document	Explicit consent (see Section 7)
Keep our systems secure	Legitimate interests. Legal obligation.
Meet record keeping, audit, Card Network and regulatory requirements	Legal obligation. Legitimate interests.
Respond to lawful requests from regulators, courts and law enforcement	Legal obligation
Establish, exercise or defend legal claims	Legitimate interests
Improve and test program services using de-identified or aggregated data	Legitimate interests

Where we rely on consent, you can withdraw it at any time. Withdrawal does not affect processing that took place before.

If you do not provide the information needed for verification, we cannot open or continue your card.

7. Biometric data

- **What we collect.** During verification we may compare a selfie or short video with the photo on your identity document. This creates a facial geometry template.
- **Why.** Only to verify your identity and prevent impersonation fraud.
- **Consent.** We ask for your explicit consent before we collect it.
- **Sharing.** Only with the Service Provider that performs the match, and as required by law. We do not sell, lease or trade biometric data.
- **Retention.** We destroy biometric templates when the verification obligations have been fulfilled.
- **Model B programs.** The Program Client is responsible for biometric consent and retention. Connect Financial receives the verification result and document images.

8. Automated decisions

We use automated tools to screen applications and transactions. Some decisions are made automatically, for example:

- Declining an application that fails identity, sanctions or risk checks
- Declining or holding a transaction that matches known fraud patterns
- Freezing a card when unusual activity is detected

These decisions help us meet legal obligations and protect you and the program.

9. Marketing

- Connect Financial does not send marketing to cardholders in Program Client programs.
- The Program Client may send you marketing under its own privacy notice and your preferences.
- We send service messages such as transaction alerts, security codes and service messages. You cannot opt out of these while your card is active. These messages may be sent by us or one of our vendors on our behalf.

10. Who we share your data with

We share personal data only as needed for the purposes in Section 6.

Recipient	Why we share
Issuing Bank	To open and operate your card account, and for the bank's own regulatory obligations
Program Client	To operate the program, provide the service in its app, support you, and exchange verification results
Connect Financial group companies	To provide shared operations, compliance, security and support services, under intragroup agreements
Card Network	To authorize, clear and settle transactions, resolve disputes, manage tokens and meet network rules
Merchants and their payment providers	Through the Card Network, to verify transactions and resolve disputes and chargebacks
Digital wallet providers	To verify and add your card when you add it to a digital wallet
Card processing and tokenization providers	To process transactions, secure card data, and provide white-label cardholder support on our behalf

Recipient	Why we share
Identity verification, fraud prevention and screening providers	To verify identity, screen against sanctions and watch lists, and prevent fraud
Payment and payout providers	To move funds to and from your card, where your program supports this
Card production and delivery providers	To produce and send physical cards
Hosting, communications and support providers	To host our systems, send messages and support you
Professional advisers, auditors and insurers	For legal, audit, compliance and insurance purposes
Regulators, law enforcement, courts and tax authorities	Where required by law, or to protect rights and safety
A buyer or successor	In a merger, acquisition or sale of assets, under confidentiality terms

Service Providers act on our instructions under written contracts that require confidentiality and security.

We do not sell your personal data. We do not share it for cross-context behavioral advertising.

11. International transfers

Connect Financial and the other parties in your program operate in several countries. Your data may be processed outside the country where you live.

Where the law requires, we protect transfers with:

- Adequacy decisions. The European Commission and the UK recognize Canada as adequate for organizations subject to PIPEDA.
- Standard contractual clauses approved by the European Commission, including intragroup agreements between Connect Financial group companies
- The UK International Data Transfer Agreement or Addendum

You can ask us for a copy of the relevant safeguards.

12. How we protect your data

- Full card numbers are handled in a tokenized, PCI DSS compliant environment operated by our card data Service Providers. Connect Financial systems do not store or display full card numbers.
- Data is encrypted in transit and at rest.
- Access is role based and limited to what each person needs. Multi-factor authentication is required for system access.
- Systems are logged and monitored.
- Service Providers are assessed before and during engagement.
- Staff are trained and bound by confidentiality.
- We maintain an incident response plan.

What you can do

- Keep your PIN, passwords and one-time codes private. Connect Financial and the Program Client will never ask for your PIN or full card number by phone, email or text.
- Secure the device you use to access your card.
- Report a lost or stolen card, or a transaction you do not recognize, to your Program Client straight away.

No system is fully secure. If a breach affects your data, we will notify you and the relevant authorities as the law requires. We coordinate notices with the Issuing Bank and the Program Client.

13. How long we keep your data

We keep data only as long as needed for the purposes in this notice, including legal and regulatory requirements. Where more than one period applies, we keep the data for the longest period.

Record	Retention period
Identity verification and due diligence records	At least 5 years after your card relationship ends, or longer where the law requires
Transaction records	At least 5 years after the transaction
Sanctions screening and suspicious activity records	At least 5 years
Biometric templates	See Section 7

At the end of the period we delete or anonymize the data. If the law requires us to keep data after you ask us to delete it, we restrict its use to that legal purpose.

14. Your rights

Depending on where you live, you may have the right to:

- Know what personal data we hold and get a copy
- Correct inaccurate data
- Delete your data
- Restrict or object to how we use it
- Receive your data in a portable format
- Withdraw consent
- Ask for human review of an automated decision
- Complain to a data protection authority

How to make a request

- Email compliance@connect.financial.
- Or contact your Program Client, which will pass the request to us.
- We verify your identity before we act.
- For data we handle on behalf of the Issuing Bank or the Program Client, we pass your request to them or act on their instructions.
- An authorized agent can make a request for you where the law allows.
- We respond within the period the law sets. For example: one month in the EU and UK, 45 days in California, 30 days in Canada. We will tell you if we need an extension the law allows.
- Requests are free, unless they are clearly unfounded or excessive.

Limits

- We may not be able to delete data we must keep under anti-money laundering or other laws.
- We may be prohibited from telling you about some investigations or reports to authorities.

We will not treat you differently for exercising your rights.

15. Regional information

15.1 European Union, European Economic Area and United Kingdom

- **Legal entity.** Connect Financial acts as controller or processor as set out in Section 3. For activities Connect Financial performs for the Issuing Bank, the Issuing Bank is the controller. Connect Fintech Services, Inc. (doing business as Connect Financial), 490-1 Bow Valley Square 3, 255 5th Avenue SW, Calgary, Alberta, Canada.
- **Legal bases.** See Section 6. Biometric data is special category data. We rely on your explicit consent for it.
- **Transfers.** See Section 11.
- **Complaints.** You can complain to the supervisory authority where you live or work, or where the issue took place. In the UK this is the Information Commissioner's Office.

15.2 United States

Financial privacy. Your card account is a financial product. The Issuing Bank's privacy notice, provided under the Gramm-Leach-Bliley Act, explains how the Issuing Bank shares your nonpublic personal information and any right you have to limit that sharing. Connect Financial handles that information as a service provider to the Issuing Bank and follows the same limits. If this notice conflicts with the Issuing Bank's financial privacy notice on that information, the Issuing Bank's notice controls.

State privacy laws. Most data in this notice is covered by the Gramm-Leach-Bliley Act and is exempt from state consumer privacy laws such as the California Consumer Privacy Act (CCPA). Where state laws apply, for example to device data or to business representatives, this section applies.

California notice at collection. In the past 12 months we collected these categories:

- Identifiers
- Customer records under California Civil Code section 1798.80(e)
- Protected classification characteristics (age, gender)
- Commercial information (transactions)
- Biometric information
- Internet or other electronic network activity
- Geolocation data
- Professional information (business representatives)
- Audio information (call recordings).
- Sensitive personal information: government identifiers, account login, biometric information.

Sources are in Section 5. Purposes are in Section 6. Recipients are in Section 10. Retention is in Section 13. We do not sell or share personal information. We use sensitive personal information only for purposes the California regulations permit, such as verifying identity and preventing fraud.

California rights. You can ask to know, delete and correct your personal information. Make a request using Section 14.

Biometric laws. Illinois, Texas, Washington and other states have specific biometric rules. See Section 7.

Other states. Residents of other states may have similar rights. Many of these laws exempt financial institutions or data covered by the Gramm-Leach-Bliley Act. If we deny your request, you can appeal by replying to our decision. If we deny your appeal, you can contact your state Attorney General.

15.3 Canada

- Connect Financial is headquartered in Calgary, Alberta. We comply with the Alberta Personal Information Protection Act (PIPA) and the Personal Information Protection and Electronic Documents Act (PIPEDA), and with other provincial laws where they apply.
- Some processing, such as verification and reporting under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, is required by law.
- **Privacy officer.** Phantom Compliance (compliance@connect.financial).
- Your data may be stored or processed outside Canada by our Service Providers and other parties in your program. It may be accessible to courts and authorities in those countries under their laws.
- We respond to access requests within 30 days, or within any extension the law allows.
- **Breach notification.** Where a breach creates a real risk of significant harm, we notify you, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada, as the law requires.
- **Complaints.** You can complain to the Office of the Information and Privacy Commissioner of Alberta, the Office of the Privacy Commissioner of Canada, or the privacy commissioner in your province.

16. Minors

Cards are not available to anyone under 18, or under the age of majority where they live. We do not knowingly collect data about children. If we learn that we have, we delete it unless the law requires us to keep it.

17. Changes to this notice

We review this notice at least once a year. If we make a material change, we will tell you before it takes effect, through the Program Client, by email or by in-app notice. The "Last updated" date shows the current version.