



## Risk & Compliance

This document provides in-depth details as to the process and procedures that are part of the day-to-day operations of eFraud Prevention, LLC.

---

Security measures in place to protect access to the content.

### Access:

- All servers and computer systems require complex password and two-factor authentication.

### Password Policy:

- Passwords are changed every 60 days.

### Intrusion Protection:

- **Firewalls:** Firewalls are in place outside of the server as well as within the server environment.
- **Patches / Updates:** All software updates are set to install automatically.
- **Anti-Virus:** Set at both the network and at the server level.
- **Denial of Service:** Set at the network level.
- **3<sup>rd</sup> Party Intrusion & Penetration testing:** Performed daily.

### Content Integrity:

- **Content:** Data and stored in multiple cloud locations as well as in a cold storage location for redundancy and security. Content is monitored every hour using server-side software and every 5 minutes using a 3<sup>rd</sup> party service to provide us with alerts if any unintended content changes occur.

## Service level agreement:

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	Service Credit for each Service Period
Availability of the Service	Availability	99.99%	98%	5% Service Credit gained for each percentage under the 98% Service Level Performance Measure

## Content Creation:

Content is written “in-house” by reviewing the most current advice from online resources, in person conferences and through discussions with industry professionals. These sources include:

- Federal Trade Commission
- Department of Homeland Security
- Department of Commerce
- U.S. Department of Education
- U.S. Department of State
- U.S. Department of Treasury - FINCEN
- Consumer Financial Protection Bureau
- CT Commission on Woman, Children & Seniors
- Federal Communications Commission
- Federal Deposit Insurance Corporation
- Information Assurance Support Environment
- Internal Revenue Service
- Securities and Exchange Commission
- United States Postal Inspection Service
- Various Offices of Secretary of State
- UK's National Reporting Centre for Fraud
- Consumer Federation of America
- SANS Institute
- OWASP Internet of Things Project
- NCEA
- National Council on Aging
- CDC
- National Adult Protective Services Association
- IAFCI – International Association of Financial Crimes Investigators
- ACAMS
- Private Cyber Security Firms
- Fraud Investigators throughout the U.S.

## Additional Disclosures:

- eFraud Prevention, LLC services do not involve critical operation activities or shared services, such as internal audit and information technology, or any activities that could cause a Financial Institution to face risk if our service fails to meet expectations. In addition, our services only provide information that pertains to preventing fraud, no financial advice is included nor any other information that that could adversely impact a bank's customer or a credit union's member, or that could damage banking operations if the Financial Institution has to find another vendor to bring the function.
- eFraud Prevention, LLC services do not include identity protection, debt collection programs or any other program that collects personal information or charges a fee to consumers.
- eFraud Prevention, LLC does not offshore any function of its business operations, services, content creation, IT, hosting or personnel.
- eFraud Prevention, LLC content creation and product development personnel have over 25 years of IT and fraud related experience and training.
- eFraud Prevention, LLC only publishes content that it creates or is available through public license. No intellectual property licenses or copyrights are infringed.
- eFraud Prevention, LLC does not engage directly with the customer or member of the Bank or Credit Union.
- eFraud Prevention, LLC does not collect or store any personal or financial information through its services to the Financial Institution.

### **How eFraud Prevention, LLC uses Client information**

We use only use information in the file we maintain about you, to provide to you the services offered by the Site; resolve service and billing disputes; troubleshoot problems; bill any amounts due from you; measure consumer interest in our products and services, inform you about online and offline offers, products, services, events and updates; deliver information to you that, in some cases, is relevant to your interests, such as product news; customize your experience; detect and protect us against error, fraud and other criminal activity; enforce our Terms of Use; provide you with system or administrative messages, and as otherwise described to you at the time of collection.

We may also use personal information about you to improve our marketing and promotional efforts, to analyze Site usage, to improve our content and product offerings, and to customize the Site's content, layout, and services. These uses improve the Site and better tailor it to meet your needs, so as to provide you with a smooth, efficient, safe and customized experience.

**eFraud Prevention, LLC disclosure of Client information:**

We will not share your personal information with third parties. We do not sell your personal information to third parties.

**Third party links:**

All third-party links from eFraud Prevention, LLC to a third-party site have a LEAVING SITE NOTICE published with the additional step of approval and consent before leaving eFraud Prevention, LLC site.

**Strategic purposes of eFraud Prevention, LLC services:**

Reduce costs, leverage specialized expertise, expand communications, comply with regulatory recommendations as they pertain to fraud education awareness.

**Employees:**

Credit union management and employees do not require training or additional time to manage Provider services.

**Conflict of interest:**

eFraud Prevention, LLC does not offer any service that conflicts or competes with the Financial Institutions.

**Proofing Process:****Grammar and format:**

We ensure that all grammatical errors are fixed by using both human and computer programs so that correct grammar is consistently used throughout our articles. Content is reviewed and proofed prior to going live on the portal.

**Implementation:**

New content is reviewed for importance and urgency, articles are written or updated and implemented as soon as they are deemed comprehensive and easy to understand by the non-technical consumer.

**External link testing:**

All external links are reviewed and vetted to ensure their site is secure and their company is a reputable organization. In addition, we make sure that any external agency or company does not offer third party services, offer advertising, link to sites that are deemed inappropriate, or advertise a service that would compete with our clients.

**Attribution and copyright:**

All content can be used without express authorization or attribution by a financial institution, the members and customers of a financial institution or the by public as a whole.

**Client feedback:**

If an eFraud Prevention client identifies contents as not being accurate or needs to be amended, we have a secure form in which this information can be sent to us for review. The review process takes place within two hours of receiving the request and content would be remedied within the same day as the request.