INFORMATIONSBLATT

RAIFFEISEN ONLINE BANKING-DIENST, CBILL-DIENST und CBI-DIENST

INFORMATIONEN ZUR BANK

RAIFFEISENKASSE PRAD-TAUFERS GENOSSENSCHAFT
KREUZWEG 8 - 39026 - PRAD AM STILFSERJOCH
Tel: 0473/619200
Fax: 0473/616611
E-Mail: rk.prad-taufers@raiffeisen.it
PEC: pec08183@raiffeisen-legalmail.it
Webseite: www.raiffeisen.it/prad-taufers

Eintragungsnummer im Bankenverzeichnis bei der Banca d'Italia: 3700.2.0
dem Einlagensicherungsfonds der Genossenschaftsbanken und dem Nationalen Garantiefonds laut Art. 62 LD Nr. 415/96 angeschlossen
Mitglied des institutsbezogenen Sicherungssystems Raiffeisen Südtirol IPS

WAS IST DER RAIFFEISEN ONLINE BANKING-DIENST, CBILL-DIENST UND CBI-DIENST

Diese Dienste ermöglichen es dem Kunden, mittels Internet Informationen abzufragen und einzelne Bankdienstleistungen in Anspruch zu nehmen, und zwar als Alternative zu den üblichen Kanälen. Zu diesem Zweck nutzt der Kunde Geräte, die mit jenen der von der Bank bei Bedarf zur Verfügung gestellten kompatibel sind und mit welchen er auf eigene Kosten eine telematische Verbindung mit der Bank einrichtet.

Die Raiffeisen Online Banking-Dienste kann der Kunde für die Geschäftsbeziehungen nutzen, die er bei der Bank unterhält. Der Dienst kann auch als "Light Version" mit weniger Funktionen unterschrieben werden.

Die CBI-Dienste des Konsortiums Corporate Banking ermöglichen dem Kunden, verschiedene Funktionen auf all seinen Geschäftsbeziehung mit jedweder Bank zu nutzen, die dem Interbankenabkommen beigetreten ist.

Der CBI F24-Dienst ist den Patronaten und Wirtschaftsberatern vorbehalten und ermöglicht es diesen, Zahlungen von F24 Modellen mit direkter Belastung der Kontokorrente ihrer Kunden durchzuführen, unter der Voraussetzung, dass sie von ihrem Kunden eine entsprechende Vollmacht erhalten haben.

Der CBILL-Dienst ermöglicht es dem Kunden Rechnungen elektronisch einzusehen und zu bezahlen, die von einem diesem Dienst beigetretenen Rechnungsaussteller ausgestellt wurden.

Die Nutzung dieser Dienste **setzt voraus**, dass der Kunde ausreichende Kenntnisse hat, um die Sicherheit des Internetzugriffes über die eigenen Geräte (PC, Tablet, Smartphone) zu gewährleisten.

Die **Hauptrisiken** dieser Dienste bestehen darin, dass der Kunde, trotz Anwendung der besten Sicherheitsmaßnahmen der aktuellen Technologie von Seiten der Bank, Opfer eines Betruges durch elektronische Mittel wird, der z.B. den Diebstahl der Zugangsdaten, das Erstellen einer Bildschirmkopie, die veränderte Darstellung von Webseiten zwecks unrechtmäßiger Aneignung des Passworts und die Fernsteuerung des Computers bewirkt. Es kann außerdem vorkommen, dass die ordentliche Abwicklung der Dienste wegen zeitweiliger Unterbrechung oder Aussetzung des Dienstes selber nicht möglich ist, sodass der Kunde für eine bestimmte Zeit weder Datenflüsse erhalten noch versenden kann.

Um diese Risiken einzuschränken sind einerseits im Raiffeisensystem verschiedenste **Sicherheitsmaßnahmen** umgesetzt, andererseits werden dem Kunden sichere Authentifizierungsmittel zur Verfügung gestellt. Zudem greifen **Verfügungslimits**, die der Kunde noch weiter herabsetzen kann.
Der Kunde ist verpflichtet eine der folgenden Sicherheitsmaßnahmen zu aktivieren:
"**SMS Alert**": SMS Mitteilungen an die vereinbarte Telefonnummer bei allen Zugriffen auf den Raiffeisen Online Banking-Dienst und/oder bei Bestätigung von Überweisungsausgängen.
"**E-Mail Alert**": E-Mail an die vereinbarte Adresse bei allen Zugriffen auf den Online Banking-Dienst und/oder bei Bestätigung von Überweisungsausgängen.

Es ist auf jeden Fall notwendig, dass der Kunde die Verhaltensregeln einhält, die in der "Anleitung für eine sichere Nutzung des Raiffeisen Online Banking-Dienstes, des CBILL-Dienstes und des CBI-Dienstes" beschrieben sind.

WIRTSCHAFTLICHE BEDINGUNGEN

KOSTENPOSTEN

	PREIS
Fixspesen	
Raiffeisen Online Banking und CBI	
Jahresgebühr einschließlich CBILL	0,00 Euro
Jahresgebühr einschließlich CBILL und CBI	15,00 Euro
Gebühr für jedes Lesegerät	29,00 Euro

Ende des Geschäftstages (Cut-off)	
Ende des Geschäftstages in Bezug auf den Eingang von Zahlungsaufträgen	
Kundenaufträge an	
Bankarbeitstagen	14:00:00 Uhr
Halbfeiertagen und Freitagen	10:00:00 Uhr
Für dringende Überweisungen an	
Bankarbeitstagen	14:00:00 Uhr
Halbfeiertagen und Freitagen	10:00:00 Uhr
Echtzeitüberweisung (SCT Instant Payment)	
Der Dienst kann im ROB rund um die Uhr in Anspruch genommen werden, sofern sämtliche Voraussetzungen erfüllt sind und die Funktion von der Empfängerbank angeboten wird. Diese SEPA-Echtzeitüberweisung ist unwiderruflich, da sie unmittelbar durchgeführt wird.	

Help Desk	
während der Öffnungszeiten der Bank	0039 0473 619 200
außerhalb der Öffnungszeiten der Bank	800 031 031 / 0471 064 200

RÜCKTRITT UND BESCHWERDEN

Rücktritt vom Vertrag

Beide Vertragsparteien können von diesem Vertrag jederzeit unter Einhaltung einer Vorankündigungsfrist von 1 Monat zurücktreten.
Bei Vorhandensein eines rechtfertigenden Grundes im Sinne des Verbraucherschutzgesetzes Nr. 206/2005 Artikel 33 Absatz 3 oder wenn es aus Gründen der Effizienz oder Sicherheit des Dienstes erforderlich ist, kann die Bank vom Vertrag auch ohne Vorankündigung zurücktreten, indem sie den Kunden umgehend darüber informiert.
Im Falle des Rücktritts von Seiten der Bank oder von Seiten des Kunden, ist die Bank verpflichtet, den Dienst für alle Datenflüsse durchzuführen, die bis zum Bankarbeitstag vor Wirksamkeit des Rücktritts bei ihr eingegangen sind.

Maximalfrist für die Beendigung der Vertragsbeziehung

Die Vertragsbeziehung endet mit der Wirksamkeit des Rücktritts, vorbehaltlich der Verpflichtung des Kunden die Beträge bereitzustellen, die die Bank begründeter maßen für den Abschluss offener Positionen von ihm verlangt.

Beschwerden

Der Kunde kann bei der Bank Beschwerde einreichen, auch mittels Einschreiben mit Rückantwort oder auf telematischem Wege (RAIFFEISENKASSE PRAD-TAUFERS GENOSSENSCHAFT, KREUZWEG 8, 39026 PRAD AM STILFSERJOCH, PEC08183@RAIFFEISEN-LEGALMAIL.IT, RK.PRAD-TAUFERS@RAIFFEISEN.IT, Fax: 0473/616611).
Sollte der Kunde innerhalb von 60 Tagen bzw. im Falle von Zahlungsdiensten innerhalb von 15 Bankarbeitstagen keine oder eine nicht zufriedenstellende Antwort erhalten haben, kann er binnen 12 Monaten ab Einreichung der Beschwerde einen Rekurs an das Schiedsgericht für Bank- und Finanzdienstleistungen und Operationen (ABF) stellen. Weitere Informationen über die Funktionsweise und die Verfahrensabläufe des ABF kann der Kunde auf der Homepage www.arbitrobancariofinanziario.it einsehen oder bei den Filialen der Banca d'Italia oder der Bank nachfragen.
Der Kunde kann zudem - allein oder gemeinsam mit der Bank - ein Schlichtungsverfahren einleiten, um eine Einigung zu erzielen. Genannter Schlichtungsversuch wird von der Bankenschlichtungsstelle (Conciliatore Bancario Finanziario - Associazione per la soluzione delle controversie bancarie, finanziarie e societarie - ADR; www.conciliatorebancario.it), angestellt.
Die vorherige Inanspruchnahme eines Verfahrens zur außergerichtlichen Streitbeilegung (Mediation bei einer beliebigen dazu ermächtigten Stelle, Mediation bei einer dazu ermächtigten und im Vertrag vereinbarten Stelle oder genanntes Verfahren beim Schiedsgericht für Bank- und Finanzdienstleistungen und Operationen-ABF) ist im Sinne des Art. 5 Abs. 1-bis des Legislativdekrets Nr. 28/2010 verpflichtend, sollte der Kunde beabsichtigen, für einen über die Auslegung und Anwendung des Vertrages entstehenden Streitfall das ordentliche Gericht anzurufen; dies bei sonstiger Unverfolgbarkeit der Klage. Das Mediationsverfahren wickelt sich vor der örtlich zuständigen Mediationsstelle und mit dem Beistand eines Rechtsanwaltes ab.

BEGRIFFSERKLÄRUNG

Aktivbank	Bank, die den CBI-Dienst anbietet, die korrekte Versorgung mit diesem gewährleistet, die Verbindung mit dem Kunden realisiert und verwaltet.
App	Kürzel für "application"; bezeichnet eine Software, die auf mobilen Geräten wie Smartphone und Tablet genutzt werden kann.
CBI	Markenbezeichnung des Anbieters Corporate Banking Interbancario.
CBI-Dienst	Der Dienst "Corporate Banking Interbancario", der aus den Funktionen besteht, die auf der Internetseite des Konsortiums CBI (www.cbi-org.eu) veröffentlicht sind.
CBILL	Produktbezeichnung für den Dienst e-Billing des Anbieters Corporate Banking Interbancario.
e-Billing	Abkürzung des englischen Begriffs "electronic billing", der Rechnungen beschreibt, die über einen telematischen Kanal übermittelt und bezahlt werden.
F24 Auftrag	Zahlungsverfügung von Steuern, Abgaben, Zulagen, Versicherungsbeiträgen.
Internetnetz	Verbindungssystem zwischen Computern, welches die weltweite Datenübermittlung erlaubt.
Lesegerät	Eines der Mittel (Identifizierungsmittel), mit denen der Kunde sich in der Anwendung selbst in seiner Geschäftsbeziehung mit der Bank ausweist.
Passivbank	Bank, die mittels der Aktivbank oder eines Zahlungsinstituts die Datenflüsse mit dem Kunden austauscht.

Raiffeisen

Anleitung für eine sichere Nutzung der Raiffeisen Online Banking-, CBILL- und CBI-Dienste

Das gegenständliche Dokument bildet integrierenden Bestandteil des Vertrages zur Nutzung des Raiffeisen Online Banking-Dienstes, des CBILL-Dienstes und des CBI-Dienstes.

Bei den Diensten, die den telematischen Zugriff auf Geschäftsverbindungen ermöglichen, wendet die Bank die besten Maßnahmen der aktuellen Technologie an, greift auf verschiedenste Sicherheitsmaßnahmen zurück und stellt sichere Authentifizierungsmittel zur Verfügung. Trotz alledem ist es möglich, dass der Kunde Opfer eines Betruges durch elektronische Mittel wird. Folglich ist es, zusätzlich zu den von der Bank getroffenen Sicherheitsmaßnahmen erforderlich, dass der Kunde über ausreichende Kenntnisse verfügt, um den Internetzugang über das eigene Gerät sicher zu gestalten.

Das Hauptrisiko besteht darin, dass der Kunde Opfer eines Hackerangriffes werden kann, welcher über das vom Kunden verwendete Gerät erfolgt und z.B. den Diebstahl der Zugangsdaten, das Erstellen einer Bildschirmkopie, die veränderte Darstellung von Webseiten zwecks unrechtmäßiger Aneignung des Passworts und die Fernsteuerung des Computers bewirkt.
Es kann vorkommen, dass der Kunde eine E-Mail Nachricht erhält, welche die Graphik der Webseite der Bank imitiert. Diese Mail, welche zum Ziel hat, das Password des Kunden abzufragen, mit welchem die Zahlungen autorisiert werden, lädt den Empfänger der E-Mail ein, einem in der Nachricht enthaltenen Link zu folgen. Dieser Link führt dann allerdings nicht auf die offizielle Webseite der Bank, sondern auf eine gefälschte Seite, welche der offiziellen sehr ähnlich ist, sich aber auf dem von einer anderen Person kontrollierten Server befindet. Diese Art von Betrug über Internet, "Phishing" genannt, kann auch über den Versand einer SMS durchgeführt werden. Diesbezüglich wird darauf aufmerksam gemacht, dass die Bank nie Mitteilungen (E-Mail oder SMS) versendet, in denen sie den Kunden auffordert, seine Zugangsdaten einzugeben.

Zudem gibt es noch unterschiedliche Angriffsformen, die darauf abzielen, den Computer mit einem Schadprogramm zu infizieren (sogenannter Banking Trojan). Dies kann auf verschiedenste Art und Weise, wie z.B. mittels einer E-Mail mit Anhängen, eines in einer E-Mail enthaltenen Links, welcher auf eine infizierende Webseite führt oder einfach über das Aufrufen einer manipulierten Webseite (sogenannter drive-by-download) erfolgen. Üblicherweise wird der Banking Trojan definitiv auf der Festplatte des Computers installiert. Es gibt aber auch andere Arten von Schadprogrammen, die sich im Systemspeicher des Computers befinden und somit auf der Festplatte keine Spuren hinterlassen. Ist das Schadprogramm einmal auf dem Computer aktiv geworden, stehen der kriminellen Organisation verschiedene Techniken zur illegalen Datenabfrage zur Verfügung, wie z.B. das Abfangen der Eingabefelder (Passwort oder Kreditkartendaten), die Darstellung von manipulierten Webseiten, die Blockierung des Zugangs zum Dienst, die Veränderung der Verbindung zwischen Webadresse und IP-Adresse, die Deaktivierung von installierten Antivirusprogrammen, die Veränderung der eingegebenen Daten (z.B. im Zuge einer Überweisung) und sogar die Fernsteuerung des Computers.

Aus diesen Gründen ist erforderlich, alle vorbeugenden Maßnahmen zu treffen, die die Durchführung von Aufträgen in einer infizierten Umgebung mit potentiellem Risiko eines Schadprogramms vermeiden. Es wird davon abgeraten, Aufträge mit einem nicht bekannten Gerät durchzuführen (z.B. Verwendung eines PCs in einem Internetcafé). Wird der Auftrag von einem eigenen elektronischen Gerät aus durchgeführt, ist es erforderlich, vor Zugriff auf die telematischen Dienste zu prüfen, ob das Gerät über ein mit allen Sicherheitspatches aktualisiertes Betriebssystem, über die aktuellsten Versionen der Benutzersoftware (z.B. Acrobat Reader) und über ein ständig aktualisiertes Antivirusprogramm verfügt.

Die genannten Voraussetzungen bilden Mindestvorkehrungen, die für eine wirksame Abwehr von eventuellen Hackerangriffen unverzichtbar sind. Es ist außerdem wichtig, dass der Kunde mit der Bank uneingeschränkt zusammenarbeitet und, vor allem im eigenen Interesse, dazu beiträgt, derartigen Angriffen vorzubeugen, indem er folgende Verhaltensregeln befolgt.

Die Bank kann den Zugang zum Dienst verwehren, wenn das Gerät des Kunden den technischen Mindestanforderungen gemäß dem Handbuch nicht entspricht.

Im Allgemeinen ist es erforderlich,

- ein aktives und stets aktualisiertes Antivirusprogramm und entsprechende Firewall zu installieren;
- auf den Dienst von eigenen Geräten aus zuzugreifen, die periodisch kontrolliert werden;
- das eigene Gerät mit einem Passwort von mindestens acht Zeichen, die nicht problemlos der Person zugeordnet werden können, zu schützen und dieses mindestens halbjährlich zu ersetzen;
- regelmäßig die Kontoauszüge und die über die Internetdienste ausgeführten Aufträge zu kontrollieren.

In Bezug auf die Nutzung des Dienstes ist es notwendig:

- die Authentifizierungsmittel mit höchster Sorgfalt zu verwahren und zu verwenden;
- einzelne Teile der Authentifizierungsmittel nicht gemeinsam aufzubewahren;
- die Authentifizierungsmittel nicht an Dritte weiterzugeben;
- den Diebstahl, den Verlust, die Zerstörung oder jegliche andere nicht erlaubte Verwendung des Zahlungsmittels und/oder der Authentifizierungsmittel zu melden;
- auf die verschiedenen Arten von potentiellen Hackerangriffen zu achten, unter anderem auf gefälschte E-Mails, gefälschte Mitteilungen bezüglich Ablauf von Fristen, die Aufforderung einen bestimmten Link zu verfolgen;

Es wird empfohlen, die Zugänge zum Dienst und die erteilten Aufträge mittels des SMS- und/oder E-Mail-Alert Dienstes zu überprüfen.

Zum Zeitpunkt des Zugangs zum Dienst ist es notwendig:

- die von der Bank im Handbuch erteilten Anweisungen zu befolgen;
- zu kontrollieren, ob das Internetprotokoll "https" und das Symbol des Schlosses, welche charakteristisch für eine geschützte Webseite sind und sich vom Internetprotokoll "http" unterscheiden, in der Status- bzw. Adressleiste aufscheinen;
- den Dienst nicht mehr zu nutzen und die Bank umgehend zu informieren - auch über die Grüne Nummer, welche auf der Webseite veröffentlicht ist - falls Unregelmäßigkeiten oder mangelnde Funktionstüchtigkeit des Systems festgestellt werden;
- nach Ausführung der Aufträge die Anwendung mittels des entsprechenden Schaltknopfes ("verlassen") schließen.

Für Unternehmen ist es außerdem notwendig:

- auf den Dienst von professionell verwalteten Arbeitsplätzen aus zuzugreifen;
- im Bereich der Sicherheit bezüglich der Nutzung der Internet Banking-Dienste eine Unternehmenspolitik zu definieren und zu verbreiten;
- die zur Nutzung des Internet Banking-Dienstes ermächtigten Personen festzulegen und ihre Zugangsprofile zu verwalten;
- innerhalb des Unternehmens für die ermächtigten Nutzer des Internet Banking-Dienstes periodische Informations- und/oder Bildungsveranstaltungen zum Thema Sicherheit zu organisieren;
- die ermächtigten Nutzer über die Kommunikationskanäle mit der Bank zu informieren, um eventuelle Anomalien/Leistungsunfähigkeiten, welche bei der Durchführung der Aufträge festgestellt werden, schneller abwickeln zu können und zeitnah Verhaltensanweisungen und Angaben zur Anwendung angemessener Maßnahmen zu erhalten;
- das Surfen im Internet und die Möglichkeit, Programme zu installieren deren Herkunft nicht festgestellt werden kann, einzuschränken;
- die Nutzerprofile auf Grundlage des Handlungsbedarfs zu unterscheiden und auf den einzelnen Arbeitsplätzen die Administratorenrechte einzuschränken/ zu entfernen - als Alternative alle Bankbewegungen von einem PC aus auszuführen, auf welchem die Verwendung der elektronischen Post und das Surfen im Internet besonders streng definiert und kontrolliert sind;
- die Mindestanforderungen an Sicherheit einzuhalten, wie sie von den gesetzlichen Datenschutzbestimmungen vorgeschrieben sind.