**ПАМЯТКА**
**по безопасности при использовании дистанционных каналов взаимодействия клиента с ООО МКК «ГФК»**

Являясь клиентом ООО МКК «ГФК», вы имеете возможность совершать денежные операции (получать и погашать займы, оплачивать услуги), получать информацию о текущей задолженности и обмениваться документами и сведениями через дистанционные каналы обслуживания, к которым относятся:

- Личный кабинет Клиента;
- Контактный Центр (горячая линия, электронная почта).

Использование дистанционных каналов взаимодействия сопряжено с риском получения несанкционированного доступа к конфиденциальной информации Клиента и оперирование денежными средствами неуполномоченными лицами.

- К конфиденциальной информации Клиента относится:
- информация об остатках денежных средств на лицевых счетах;
- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных вами распоряжениях на перевод денежных средств;
- информация, о текущей задолженности;
- аутентификационные данные (логин, пароль, коды)
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации.

С целью снижения рисков получения несанкционированного доступа к конфиденциальной информации Клиента рекомендуем учитывать следующее:
Передача карты или ее реквизитов, Логина (Идентификатора пользователя), Постоянного пароля, Одноразовых паролей, предназначенных для доступа и подтверждения операций по дистанционным каналам обслуживания, другому лицу означает, что вы предоставляете возможность другим лицам распоряжаться вашими данными.
При любых подозрениях на мошенничество следует незамедлительно обратиться на горячую линию ООО МКК «ГФК» по номеру телефона 88003334788.

**Меры безопасности при использовании карты**
Храните свою карту в недоступном для окружающих месте. Не передавайте карту и ее реквизиты другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, удостоверяющих личность, особенно в поездках.
Во избежание мошенничества с использованием Вашей карты требуйте проведения операций с картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения.
Во избежание использования Вашей карты третьим лицом храните ПИН отдельно от карты, исключив одновременный доступ к ним (например, в одном бумажнике), не пишите ПИН на карте, не сообщайте ПИН другим лицам (в том числе родственникам), не вводите ПИН при работе в сети Интернет.
Ни при каких обстоятельствах не сообщайте свой ПИН никому.

**Меры безопасности при работе с личным кабинетом**
Для последующего входа в личный кабинет (после первичного прохождения регистрации) вам необходимо ввести Логин (Идентификатор пользователя) и Постоянный пароль. Храните эти данные в недоступном для посторонних месте. Помните, что зачастую злоупотребляют вашим доверием люди, имеющие доступ к вашему Мобильному устройству, банковской карте и паспортным данным.

При получении от ООО МКК «ГФК» на Мобильное устройство SMS-сообщения и/или Push-уведомления с Одноразовым паролем внимательно ознакомьтесь с информацией в сообщении/уведомлении: все реквизиты операции в направленном Вам сообщении/уведомлении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того, как Вы убедились, что информация в этом SMS-сообщении/Push-уведомлении корректна, можно вводить пароль.
Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашим персональным данным.

Для исключения компрометации вашей финансовой информации и персональных данных настоятельно не рекомендуем Вам подключать к личному кабинету номера телефонов, которые Вам не принадлежат.

На Мобильных устройствах, которые Вы используете для доступа к сайту glavfinans.ru:

- используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;
- регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты Вашего Мобильного устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.
- своевременно устанавливайте доступные обновления операционной системы и приложений на Ваше Мобильное устройство. Используйте антивирусное программное обеспечение для Мобильного устройства, своевременно устанавливайте на него обновления антивирусных баз.
- не устанавливайте на свое Мобильное устройство нелицензионные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате Ваше Мобильное устройство становится уязвимым к заражению вирусными программами.
- установите на Мобильном устройстве пароль для доступа к устройству, данная возможность доступна для любых современных моделей Мобильных устройств.