

Антифрод центр: первые результаты борьбы с финансовым мошенничеством

Антифрод-центр Национального банка Казахстана — это специализированная платформа, созданная для противодействия финансовому мошенничеству при платежах и переводах и для повышения безопасности всей финансовой системы. Благодаря обмену информацией между банками, платежными организациями и государственными органами центр позволяет оперативно реагировать на подозрительные активности и блокировать такие операции до того, как средства попадут к злоумышленникам.

Когда создан Антифрод-центр и для чего?

Антифрод-центр Национального банка Республики Казахстан создан в июле 2024 года для выявления и предотвращения мошеннических транзакций: от фиксации инцидента до блокировки подозрительных операций и возврата средств. Также центр обеспечивает круглосуточный обмен данными между финансовыми организациями, мобильными операторами и правоохранительными органами для быстрой реакции на подозрительные активности. Благодаря такому обмену формируются базы данных, включающие «черные» и «серые» списки подозрительных транзакций и карт/счетов, что помогает быстрее распознавать типичные схемы мошенничества.

Сегодня платформа объединяет более **250** участников. Это банки, МФО и правоохранительные органы. Они работают в одном информационном пространстве, чтобы оперативно предотвращать мошенничество и расследовать преступления. Помимо банков и МФО, к платформе подключаются игроки цифрового рынка, включая сотовых операторов.

Первые результаты

С момента запуска в системе зарегистрировано более **80 000** инцидентов, около половины из них поступили от финансового рынка, вторая часть от МВД и правоохранительных органов. По данным Антифрод-центра, наибольшую долю составляют **5** видов мошенничества:

1. Ложные звонки — классическая социальная инженерия.
2. Фиктивные онлайн-магазины — чаще всего при покупках в Instagram и на маркетплейсах.
3. Лжеинвестирование — реклама сверхдоходности без реальных оснований.
4. Мошенничество в социальных сетях — взломанные аккаунты, просьбы «занять» или перейти по ссылке.
5. Кредитное мошенничество — часто производное от ложных звонков или фейковых инвестиций.

Эти пять категорий формируют **81%** всех зарегистрированных случаев.

По итогам работы Антифрод-центра:

- **1,9 млрд** тенге сохранены на счетах отправителей;
- **400 млн** тенге сохранены на счетах получателей в ожидании возврата;
- **461 млн** тенге уже возвращены пострадавшим.

Кто становится жертвой? Портрет пострадавшего.

Портрет пострадавшего различный и он зависит от множества факторов. В разных регионах наиболее подверженными мошенничеству становятся даже различные возрастные группы.

Сезонность также играет роль: осенью фиксируется заметный рост инцидентов, прежде всего связанных с фиктивными онлайн-магазинами, что совпадает с увеличением цифровых покупок.

Большинство случаев связаны с суммами до 1 млн тенге, далее по частоте идут инциденты до 100 тыс. тенге. Однако в системе зафиксировано 995 случаев свыше 10 млн тенге, что указывает на разнообразие так называемых «целевых аудиторий» у мошенников.

География также широка: больше всего пострадавших в Алматы, Астане и Караганде, но инциденты отмечены по всей стране.

Однако есть и другой аспект, в котором наиболее рискованная аудитория — молодые люди 18–24 лет. Многие из них вовлекаются в схемы как «менеджеры по переводам», нередко не осознавая, что участвуют в противоправной деятельности и становятся дропперами. С учетом уголовной ответственности за дропперство участники таких схем не только вынуждены компенсировать финансовые потери жертв, но и могут получить вполне реальный срок.

Как обезопасить себя от мошенников?

Если вы стали жертвой мошенничества, незамедлительно обращайтесь в свой банк. Быстрая реакция — ключ к сохранению средств и предотвращению их вывода мошенниками.

Чтобы защитить себя, важно соблюдать простые, но эффективные рекомендации:

- Никогда не сообщайте никому коды подтверждения, пароли и данные карты — даже если звонящий представляется сотрудником банка.
- Не переходите по подозрительным ссылкам и не открывайте файлы от неизвестных отправителей.
- Устанавливайте лимиты на операции и обязательно подключайте уведомления о списаниях, чтобы сразу заметить подозрительную активность.
- Периодически проверяйте свою кредитную историю, пользуйтесь отдельной картой для онлайн-покупок и ни при каких обстоятельствах не передавайте свои карты, аккаунты или доступы третьим лицам.

Важно! Если вы заметили что-то подозрительное, немедленно блокируйте карту и связывайтесь с банком. При подтверждении факта мошенничества нужно незамедлительно подать заявление в полицию через платформу eOtinish.

И самое главное — развивайте критическое мышление. Именно оно помогает вовремя заметить несостыковки, не поддаваться давлению и не реагировать импульсивно. Чем спокойнее и осознаннее вы оцениваете ситуацию, тем меньше шансов, что мошенники смогут вас обмануть!