
Комплаенс-контроль

В настоящий момент вопросы противодействия мошенничеству являются принципиально важными как для собственников бизнеса, так и для менеджмента банков. При этом неблагоприятные условия внешней среды функционирования хозяйствующего субъекта, в том числе связанные с прошедшими и прогнозируемыми кризисными экономическими явлениями, делают особо актуальными задачи обеспечения стабильности развития кредитной организации и сохранности ее материальных и нематериальных активов.

С.В. ИЕВЕНКО, компания «Эрнст энд Янг», менеджер отдела по противодействию мошенничеству и содействию в спорных ситуациях компании, к.э.н.

И.А. ЛЕБЕДЕВ, Финансовый университет при Правительстве Российской Федерации, кафедра «Анализ рисков и экономическая безопасность», доцент, к.э.н.

Отдельные аспекты противодействия мошенничеству в кредитных организациях

Четыреста сравнительно честных способов отъема денег

Прежде чем приступить к обсуждению вопросов мошенничества и методов борьбы с этим явлением в кредитных организациях, необходимо разобраться с самим определением мошенничества. В широком смысле мошенничеством может являться любое преступление, совершаемое с целью наживы, в основе которого лежит обман. При этом нельзя считать, что обман сам по себе является мошенничеством. Для соответствия юридическому определению мошенничества необходимо наличие ущерба у пострадавшей стороны, выраженного в денежной форме. Согласно определению Ассоциации дипломированных специалистов по расследованиям мошенничеств (Association of Certified Fraud Examiners, ACFE) для классификации чего-либо как мошенничества необходимо наличие:

Отдельные аспекты противодействия мошенничеству в кредитных организациях

- существенно ложного утверждения;
- осознания того, что утверждение было заведомо ложным в момент, когда было сделано;
- доверия к данному утверждению со стороны потерпевшего;
- понесенного в результате всего этого убытка¹.

Однако в соответствии с отечественным подходом, закрепленным в нормах уголовного права Российской Федерации, под мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием². Таким образом, в российском правовом поле имеет место отграничение мошенничества от других смежных составов преступления, предусмотренных уголовным правом, например от злоупотребления полномочиями (ст. 201 УК РФ), коммерческого подкупа (ст. 204 УК РФ), присвоения и растраты (ст. 160 УК РФ), лжепредпринимательства (ст. 173 УК РФ), незаконного получения кредита (ст. 176 УК РФ), злоупотребления при эмиссии ценных бумаг (ст. 185 УК РФ), преднамеренного и фиктивного банкротства (ст. 196 и 197 УК РФ) и др. При этом в соответствии с мировой практикой противодействия мошенничеству указанные злоупотребления могут включаться в расширительное толкование понятия Fraud³.

Безусловным является тот факт, что любые организации, независимо от индустрии, в которой они осуществляют свою деятельность, не защищены от угрозы мошеннических рисков. Мошенничество в крупных размерах привело к краху многие корпорации по всему миру, нанеся им непоправимый урон в виде инвестиционных потерь, значительных издержек на ведение судебных разбирательств, публичных скандалов, связанных с заявлениями о мошеннических действиях топ-менеджмента и в отдельных случаях даже акционеров. Все это также стало ключевой причиной существенных репутационных издержек. На сегодняшний день в международной практике действует ряд законов и рекомендаций, в частности Закон США о коррупции за рубежом (FCPA), Закон Сарбейнса — Оксли о борьбе с корпоративным и бухгалтерским мошенничеством (Sarbanes-Oxley Act), Закон Великобритании «О борьбе со взяточничеством» (UK Bribery Act), основная цель которых — повысить ответственность менеджмента организаций за управление мошенническими рисками и противодействие им.

Мошенничество в крупных размерах привело к краху многие корпорации по всему миру, нанеся им непоправимый урон в виде инвестиционных потерь, значительных издержек на ведение судебных разбирательств, публичных скандалов, связанных с заявлениями о мошеннических действиях топ-менеджмента и акционеров.

¹ Уэллс Дж.Т. Справочник по предупреждению и выявлению корпоративного мошенничества. М.: «Маросейка», 2008.

² Ст. 159 Уголовного кодекса Российской Федерации.

³ Лебедев И. Особенности злоупотреблений на предприятиях ТЭК // Топливный рынок. 2010. № 16.

Комплаенс-контроль

Развитие банковской сферы сопровождается не только ростом количества и объемов мошеннических операций, но и повышением степени изощренности криминальных «танантов».

По сравнению с прочими отраслями организации кредитно-финансовой сферы в наибольшей степени подвержены рискам мошенничества. Так, согласно глобальному исследованию по вопросам противодействия мошенничеству, проведенному АСФЕ в 2010 г., именно здесь фиксируется наибольшее число мошеннических действий (более 16% от общего числа всех зарегистрированных случаев). Данная тенденция характерна, к сожалению, и для России. В самом деле, несмотря на последствия недавнего финансового кризиса, кредитно-финансовая сфера в России продолжает развиваться достаточно быстрыми темпами. Этому способствуют как объективная потребность во взаимоотношениях между хозяйствующими субъектами, так и процесс интеграции России в мировую экономику. Но у каждой медали есть обратная сторона. Развитие банковской сферы сопровождается не только ростом количества и объемов мошеннических операций, но и повышением степени изощренности криминальных «танантов», которые в целях посягательства на чужое имущество умело применяют современные компьютерные технологии, средства связи, множительную технику, технические средства незаконного получения информации и т.п.

Мошеннические преступления в кредитно-финансовой сфере поражают как своими объемами, так и многообразием всевозможных комбинаций: слова небезызвестного литературного героя Остапа Бендера о «четырёхстах сравнительно честных способах отъема денег» как нигде более применимы именно здесь (см. таблицу).

В российской банковской сфере, безусловно, есть своя шкала предпочтений в использовании тех или иных мошеннических схем, а некоторые схемы, весьма популярные сейчас на западных рынках, для нас пока остаются достаточно экзотичными. В качестве примеров таких схем можно привести:

- 1) подделывание подписей на векселях клиентов при выдаче под них займов;
- 2) мошенничество с учтенными векселями, когда изымаются уже учтенные банком векселя для повторного их учета в другом банке или даже в том же самом банке;
- 3) присваивание сотрудником банка крупных сумм денег путем использования чеков, оставленных в банке заемщиками с целью оплаты полученных кредитов по окончании срока.

Существует также и ряд схем, широко используемых как зарубежными, так и отечественными мошенниками, в частности:

— мошенничество при расчетно-кассовом обслуживании (безвозвратная недостача денежных средств с (без) фабрикацией(и) денежных

Отдельные аспекты противодействия мошенничеству в кредитных организациях

Таблица

Структура мошеннических схем, применяемых в банковско-финансовой сфере за рубежом

Вид мошеннической схемы	Количество случаев использования данной схемы	Процент от общего количества зарегистрированных случаев мошенничества
Коррупция	101	33,9
Кассовая наличность	64	21,5
Выставление счетов	37	12,4
Манипуляции с чеками	35	11,7
Безналичные расчеты	33	11,1
Копирование данных с банковской карточки	32	10,7
Присвоение имущества	29	9,7
Оплата расходов	20	6,7
Искажение финансовой отчетности	16	5,4
Операции с заработной платой	9	3,0
Регистрация кредитов	8	2,7

Источник: ACFA, Global Fraud Study, 2010.

документов, взятие денег из кассы «на время», сокрытие привлеченных депозитов через «перекрытие» старых клиентов новыми);

— подмена валюты (замена новых купюр старыми, вытягивание денег из денежных пачек);

— мошенничество с валютными операциями (злоупотребления при конвертации валют, «модернизация» компьютерной программы учета движения валютных средств банка по счетам граждан, неправильное сложение нескольких видов валют при осуществлении валютных переводов, мошенничество с дорожными чеками);

— мошенничество с выдачей кредитов (выдача кредитов под несуществующий залог, необоснованные займы фирмам, необоснованное высвобождение залога, в котором есть личная заинтересованность сотрудника банка, выдача кредита под льготный процент «своим» организациям, занижение получаемого дохода от выдаваемых ссуд);

— передача сотрудниками банка информации о своих клиентах банкам-конкурентам;

— манипуляции с ценными бумагами (утаивание части выручки от продажи ценных бумаг клиентов, умышленно неэффективная

Комплаенс-контроль

покупка ценных бумаг, изъятие ценных бумаг банка и их последующая продажа в личных целях банковским сотрудником, замена обесцененных ценных бумаг сотрудника прибыльными ценными бумагами банка);

— мошенничество со стороны бухгалтеров банка (завышение фактических процентов, начисляемых по счетам, и использование суммы завышения для компенсации фиктивных расходов; занижение комиссионных сборов по счетам клиентов с последующим зачислением полученной разницы на подставную фирму; завышение и занижение сумм проводок; использование средств временно не используемых счетов)¹.

Если же говорить о мошеннических схемах-«лидерах», которые встречаются в российских кредитных организациях, к ним прежде всего можно отнести:

- 1) мошенничество при выдаче кредита;
- 2) мошенничество при приеме депозита;
- 3) распространение внутренней информации банка (о клиентах, черных списках и пр.).

По информации, обнародованной в августе текущего года представителями российской полиции, в 2011 г. в результате ненадлежащих процедур проверки платежеспособности заемщиков, проводимых банками при выдаче кредитов, банковский сектор России недосчитался более 25,4 млрд руб. А по словам начальника главного следственного управления ГУ МВД РФ по Челябинской области Анатолия Киселева, «...практически вся российская банковская система сегодня поражена незаконным получением кредитов...»². Данные преступления, несомненно, совершаются отнюдь не без участия сотрудников кредитных организаций. Благоприятная среда для осуществления подобных схем создается, как ни странно, самими банками, которые во время бурного роста розничного кредитования и, как следствие, увеличения сетей своих продаж не только стали упрощать бизнес-процессы при кредитовании, но и ослабили требования к заемщикам с одновременным сокращением времени на принятие решения. Украсть большую сумму денег без привлечения сотрудников банка практически невозможно. Именно с их помощью мошенники, как правило, выясняют алгоритм принятия решения по выдаче кредита и процедуру проверки заемщиков. В тех случаях, когда мошеннический кредит выдается под залог, «свой» сотрудник

В числе схем, активно используемых мошенниками, можно назвать: мошенничество при расчетно-кассовом обслуживании; подмену валюты; злоупотребления при конвертации валют; мошенничество с выдачей кредитов; передачу сотрудниками банка информации о своих клиентах банкам-конкурентам.

¹ Лученок А. Справочник по нестандартным методам бизнеса и экономического мошенничества.

² <http://www.mediazavod.ru/articles/106716>

Отдельные аспекты противодействия мошенничеству в кредитных организациях

банка может серьезно зависеть его стоимость: таким образом выдача кредитных средств будет обеспечена «воздухом». Иногда мошенникам удается внедрить членов группы в кредитный департамент, и в результате их бурной деятельности конечные лица, принимающие решение о выдаче кредита, получают искаженную информацию.

Какой должна быть внутренняя программа управления мошенническими рисками?

Для того чтобы результаты борьбы с мошенничеством не были сродни результатам борьбы с ветряными мельницами, кредитной организации необходимо выстраивать комплексную программную защиту. Многие кредитные организации располагают достаточно разрозненным набором соответствующих процессов, процедур и правил. Вот только некоторые из них.

Примеры правил по предупреждению мошеннических рисков в расчетно-кассовых центрах кредитных организаций

1. Пересчет наличных денег как в кассах, так и в хранилище следует производить на регулярной основе без заблаговременного уведомления ответственных сотрудников о точной дате проверки.
2. Работники кассы не должны заниматься оформлением депозитных договоров или выпиской депозитных сертификатов, а также осуществлять бухгалтерские банковские операции.
3. Кассирам запрещается заполнять документы за своего клиента. В случае необходимости помощь в составлении документов должен оказывать специальный работник, не связанный с расчетно-кассовым обслуживанием.
4. Все операции, проходящие через кассира, должны надлежащим образом идентифицироваться как прошедшие его операционную обработку.
5. Кассирам запрещается оставлять большие суммы наличных денег на виду у посетителей или посторонних для кассы работников банка.
6. Все отправления денежных средств должны проходить проверку должностным лицом, с тем чтобы фиктивные перемещения денежных средств не могли использоваться для операции «перекрытия».
7. Недостачи или излишки, обнаруженные в кассе, должны немедленно отражаться в сводном бухгалтерском учете.
8. Жалобы клиента на расчетно-кассовый центр рассматриваются должностным лицом, непосредственно не связанным с работниками указанной структуры.

Украсть большую сумму денег без привлечения сотрудников банка практически невозможно. Именно с их помощью мошенники, как правило, выясняют алгоритм принятия решения по выдаче кредита и процедуру проверки заемщиков.

Комплаенс-контроль

Примеры правил по предупреждению мошеннических рисков в кредитных департаментах

1. Решения о выдаче кредитов должны приниматься только коллегиально на заседании кредитного комитета или аналогичного ему органа.

2. Построение системы оценки заемщиков должно быть организовано таким образом, чтобы она была известна только ключевым работникам банка.

3. Принятие решения о выдаче кредита должно быть полностью централизовано (работники фронт-офиса вводят заявку, далее проверка и принятие решения осуществляются централизованно другим персоналом).

4. Проверки отсутствия связи между работниками фронт-офиса и лицами, принимающими решение о выдаче кредита, должны проходить на постоянной основе.

МНЕНИЕ



С.Л. ЕРМАКОВ,
Институт финансового и банковского права МГЮА имени О.Е. Кутафина, доцент кафедры финансового и банковского права, действительный член (академик) РАЕН, к.э.н.

Представленный авторами перечень преступлений, совершаемых в банковской сфере, может быть расширен такими видами противоправной деятельности, как: коммерческий подкуп, контрабанда, легализация неправомочно полученных доходов и имущества, приобретенного незаконными способами, невозвращение из-за границы средств в иностранной валюте и др.

Таким образом, перечень угроз безопасности банковской деятельности от преступных посягательств довольно значителен и многообразен. Их своевременное выявление и нейтрализация являются первоочередной задачей всех субъектов экономической деятельности. Следовательно, сам вопрос требует крайне тщательного, глубокого и, пожалуй, более широкого исследования. Он может быть обозначен, скажем, как «зло-

употребления, совершаемые при проведении банковских и финансовых операций», а его исследованием и изучением должны заниматься все категории лиц, связанных с обеспечением экономической безопасности, причем на системной основе, возможно даже — на уровне государственной программы.

Как известно, произошедшие в последние десятилетия изменения в отношениях собственности и образование новой экономической реальности привели к значительным изменениям в организации работы по предупреждению преступных посягательств между государственными структурами и другими субъектами экономических отношений. Предпринимательским структурам (к которым с полной ответственностью необходимо относить и кредитно-банковские организации) приходится

Отдельные аспекты противодействия мошенничеству в кредитных организациях

5. Полномочия на установление процентных ставок и само решение о выдаче кредита должны быть разграничены.

6. Полномочия на выдачу или продление кредитов и оценка их полного обеспечения ликвидным залогом должны быть разграничены.

7. Контроль за наличием залога по выданным ссудам должен осуществляться на регулярной основе.

8. Контроль за правомерностью выдачи кредитов и установления процентных ставок должен осуществляться не реже чем раз в квартал.

9. Расходование средств со спецсудного счета клиента, взявшего кредит, должно осуществляться на постоянной основе лицами, не заинтересованными в проверке обязательств по каждому заемщику.

заниматься деятельностью, выполнение которой ранее брали на себя государственные структуры. К этому их обязывает статус собственника. Обеспечение безопасности собственной деятельности становится жизненно важной потребностью, одним из базовых принципов функционирования негосударственных хозяйствующих субъектов.

Таким образом, в современных условиях защита экономических интересов лежит на плечах не только государственных органов, но и самих предпринимателей, банкиров. Получение экономической самостоятельности предполагает и определенную долю ответственности за организацию и осуществление мер защиты своего бизнеса, в особенности — банковского.

Как следствие, назрела острая необходимость с помощью различного

рода аналитических и исследовательских работ, доступных специалистам в соответствующих сферах бизнеса, сформировать базовые представления о системе защиты банковских и финансовых операций, банковской и коммерческой тайны, информации от внутренних и внешних угроз, безотлучно сопровождающих банковскую деятельность.

Иными словами, работа по пропаганде этих знаний необходима. И не надо считать, что это — ликбез для «злодеев». Чем шире и глубже будут изучены методы и формы противоправной деятельности и борьбы с ней, тем сложнее будет преступать закон, следовательно, тем более защищенным и вооруженным будет предпринимательский (банковский) бизнес. А изощренность преступников никогда не имела границ!

Комплаенс-контроль

Примеры правил по предупреждению мошеннических рисков со стороны бухгалтеров кредитных организаций

1. Ревизии или проверки счетов опытными банковскими аудиторами должны проводиться на внезапной основе.

2. Ни один бухгалтер не должен осуществлять проводки по переводу средств с одного счета на другой ни под каким предлогом.

3. Наличие на всех проводках (кроме чеков и бланков о внесении депозита, направляемых в бухгалтерию) правомочной подписи должно постоянно контролироваться.

4. Все временно неиспользуемые счета должны находиться под контролем одного из банковских служащих из числа руководящего состава.

5. Личные счета работников бухгалтерии должны постоянно проверяться на предмет наличия необычных вкладов.

Прочие общие правила по предупреждению мошеннических рисков в кредитных организациях

1. Проверка всех нанимаемых на работу в кредитную организацию должна в безусловном порядке проводиться службой безопасности.

2. Проверка правильности выполнения обязанностей сотрудниками кредитной организации может осуществляться с помощью подставных клиентов.

Все эти правила и положения должны быть не просто собраны в единую программу. Внутренняя программа управления мошенническими рисками кредитной организации также должна включать следующие обязательные разделы:

— роли и обязанности сотрудников кредитной организации (данный раздел необходим для недопущения так называемого конфликта интересов, что особенно касается небольших банков, зачастую практикующих совмещение «конфликтных» обязанностей одним и тем же сотрудником);

— определение принципов этического поведения, а также механизмов уведомления банка его сотрудниками, клиентами и прочими сторонними организациями в случаях нарушения данных этических принципов;

— механизмы и инструменты оценки мошеннических рисков;

— система уведомления о нарушениях программы управления мошенническими рисками («горячая линия»), а также принципы защиты осведомителей;

Новейшие технологии анализа данных помогают организации выявить, насколько эффективны выстроенные ею системы внутреннего контроля, а также точно и своевременно идентифицировать транзакции с высокой вероятностью наличия мошенничества.

Отдельные аспекты противодействия мошенничеству в кредитных организациях

- процедуры расследования мошенничества;
- перечень корректирующих изменений;
- порядок последующего мониторинга.

Технологии анализа данных на службе у внутреннего контроля

Кроме того, хотелось бы обратить внимание на современные технологии анализа данных, которые помогают совершенствовать и укреплять механизмы определения мошенничества в кредитных организациях (fraud detection). Данные технологии основаны на разнообразных наборах методологий, базирующихся на методах искусственного интеллекта (artificial intelligence) и инструментах управления принятием решений (decision management). Иными словами, анализируется имеющаяся у организации статистика с целью идентификации неочевидных на первый взгляд взаимосвязей с дальнейшей обработкой этих данных таким образом, чтобы они стали не только понятны, но и полезны¹. Технологии анализа данных помогают организации выяснить, насколько эффективны выстроенные ею системы внутреннего контроля, а также точно и своевременно идентифицировать транзакции с высокой вероятностью наличия мошенничества. Указанные технологии основаны на выявлении необычных «всплесков» в совокупности анализируемых транзакций и прочей релевантной информации. В этом состоит их главное отличие от метода анализа случайной выборки, когда анализируемая популяция достаточно равномерна. Приведем несколько примеров:

- 1) все отделения кредитной организации выдают в среднем x кредитов, а одно отделение — $15x$;
- 2) средний размер кредита во всех отделениях равен $x \times 1000$ у.е., а в одном — $x \times 10\,000$ у.е.;
- 3) в связи с приходом нового сотрудника в одно из отделений кредитной организации резко выросло количество одобренных заявок на получение кредита.

Такие системы только начинают появляться в отечественных банках, но эффект от их внедрения уже очень высокий. К наиболее распространенным методикам технического анализа относятся, например, следующие:

- расчет статистических параметров (например, средних, максимальных и минимальных значений в популяции данных, а также

¹ Иевенко С., Корогодски А. Прогнозное моделирование как ключевой фактор успеха современного страхования // Современные страховые технологии. 2008. № 5.

Комплаенс-контроль

среднеквадратических отклонений) для идентификации аномальных значений, являющихся индикатором наличия мошенничества;

— анализ стратифицированных выборок с целью выявления необычных отклонений во входящих данных;

— анализ цифровых данных с использованием закона Бенфорда (Benford's Law) для выявления искусственных манипуляций с цифровыми массивами данных;

— проверка на дублирование с целью выявления повторных записей по транзакциям;

— гЭп-анализ для выявления отсутствия той или иной информации, которая априори должна быть внесена полностью;

— проверка времени ввода информации для идентификации записей, время ввода которых не характерно для внесения данных определенного вида, и т.д.

Выводы

Обобщая изложенное, полагаем возможным сделать ряд выводов:

— в настоящий момент в качестве расширительного определения понятия мошенничества используется подход, применяемый в современной западной практике и включающий в себя элементы умысла и материального ущерба, нанесенного путем обмана или злоупотребления доверием. Следует подчеркнуть, что деяния, квалифицирующиеся в качестве случаев мошенничества в соответствии с представленным подходом, не всегда могут быть признаны таковыми в соответствии с нормами уголовного законодательства Российской Федерации;

— помимо несоответствия рассматриваемых подходов, отметим, что западные мошеннические схемы не всегда эффективны в современной отечественной практике, хотя основные применяемые способы злоупотреблений совпадают. В то же время данные отличия могут быть вызваны различным трактованием одних и тех же деяний. Так, отмеченные в статье мошенничества при выдаче кредита практически невозможны без предварительного сговора с сотрудниками кредитной организации и вполне могут быть отнесены к коррупционным злоупотреблениям (внутрикорпоративная коррупция);

— наиболее эффективным образом противодействие мошенничеству может быть организовано лишь на основе использования комплексного подхода, включающего в себя, наряду с элементами выявления, механизмы расследования и предотвращения выявленных деяний в будущем. 