АНАЛИЗ СУДЕБНОЙ ПРАКТИКИ ЗА 2016 ГОД ПО СПОРАМ В РЕЗУЛЬТАТЕ ХИЩЕНИЙ ЧЕРЕЗ КАНАЛЫ ДБО

ВЫВОДЫ

1. Всего за 2016 год судами было вынесено 194 решения по спорам между банками и их клиентами в части возмещения ущерба от проведения несанкционированных транзакций с использованием систем ДБО (включая интернет–банкинг, мобильный банкинг и карты физических лиц).

2. Средняя сумма иска для юридических лиц составила 9 714 040 рублей. Средняя сумма иска для физических лиц – 421 647 рублей.

3. В 81% случаев суды отказывали клиентам в полном объеме. При этом, суды выносят решения в пользу клиентов–физических лиц в 1,5 раза чаще, чем в отношении клиентов–юридических лиц.

4. Всего за 2016 год было вынесено 31 решение по делам, где истцами выступали юридические лица. При общей сумме исков в 301 135 239 рублей, с банков удалось взыскать 32 000 рублей.

ВВЕДЕНИЕ

Данный отчет содержит анализ судебной практики по спорам между банками и их клиентами, которые произошли в результате хищений денежных средств клиентов через каналы дистанционного банковского обслуживания (далее – ДБО).

Отчет был подготовлен аналитиками Центра судебных экспертиз компании RTM Group.

RTM Group (http://www.rtm.group/) – группа экспертных и юридических компаний, специализирующихся на правовых и технических вопросах в области информационных технологий и информационной безопасности. Первый на российском рынке исполнитель судебных нормативно–технических ИТ и ИБ экспертиз.

МЕТОДИКА

В целях подготовки настоящего отчета проанализированы опубликованные данные судов общей юрисдикции и арбитражных судов РФ.

Анализ судебной практики проведен за 2016 год по данным, доступным на 16.01.2017. Статистика основывается на анализе судебных решений. Дела, которые были завершены до 01.01.2016 или решения по которым не были подготовлены до 31.12.2016, в общую статистику не включены.

В общую статистику судебных решений включены решения, подготовленные судами в рамках обжалования.

Сумма иска по делам в судах общей юрисдикции известна не по всем делам. Расчет средней суммы иска сделан только по тем делам, сумма иска по которым известна.

Сумма иска по арбитражным делам известна в полном объеме.

Критерием включения дела в статистику являлись следующие обстоятельства:

1. В решении имеется ссылка на нарушения Гражданского кодекса по статье 847.

2. В решении имеется указание на использование при списании денежных средств систем дистанционного банкинга.

3. Включение дела в одну из следующих категорий споров:
   - I. Иски о взыскании сумм по договору займа, кредитному договору;
   - II. О защите прав потребителей – из договоров в сфере торговли, услуг и т.п.;
   - III. О защите прав потребителей – из договоров с финансово–кредитными учреждениями;
   - IV. О защите прав потребителей;
   - V. О защите прав потребителей из договоров с финансово–кредитными учреждениями в сфере услуг кредитных организаций;
   - VI. О защите чести, достоинства, деловой репутации граждан и юридических лиц;
   - VII. Прочие дела особого производства;

VIII. Прочие исковые дела;
IX. Споры о возмещении вреда;
X. Споры о неисполнении или ненадлежащем исполнении обязательств по договорам банковского счета, при осуществлении расчетов;
XI. Споры о неисполнении или ненадлежащем исполнении обязательств по договорам займа и кредита;
XII. Споры о неисполнении или ненадлежащем исполнении обязательств по иным видам договоров;
XIII. Споры о неосновательном обогащении, вытекающем из внедоговорных обязательств;
XIV. Иные споры.

Дополнительная проверка проведена по делам в категориях:

- Иски о взыскании сумм по договору займа, кредитному договору;
- Споры о неисполнении или ненадлежащем исполнении обязательств по договорам займа и кредита.

В статистику включены только те дела, по которым доказывалось несанкционированное списание денежных средств с использованием каналов ДБО.

Каждое дело проанализировано на предмет соответствия критериям экспертами RTM Group. Составлен общий реестр дел с выделением следующих атрибутов:

- Дата решения;
- Категория спора;
- Суд;
- Сумма иска;
- Судья;
- Исход рассмотрения;
- Результат обжалования;
- Номер дела;
- Истец;
- Ответчик;
- Третьи лица;
- Иное лицо.

ЦЕЛЬ ИССЛЕДОВАНИЯ

Провести обобщение судебной практики за 2016 год по спорам между банками и их клиентами в результате хищений с использованием каналов ДБО.

IP

Расширенная версия настоящего отчета подготовлена для внутреннего использования компанией RTM Group и имеет отметку «ДСП».

Настоящий отчет является сокращенной версией и может быть использован неограниченным кругом лиц.

В случае использования данных из отчета третьими лица обязательна ссылка на источник.

ОСНОВНАЯ ЧАСТЬ

Всего за 2016 год судами общей юрисдикции и арбитражными судами РФ подготовлено в общей сложности 194 судебных решения.

Судами общей юрисдикции подготовлены решения по 163 делам, Арбитражными судами по 31 делу.

Распределение количества дел по типу клиента представлено на рисунке 1.

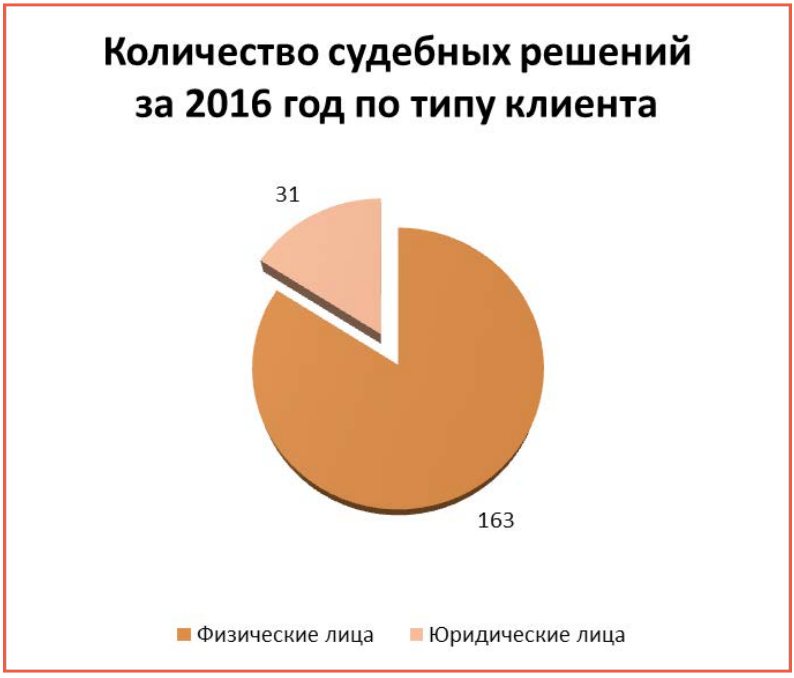

Рисунок 1.
Распределение количества дел по типу клиента

Из общего количества в 194 дела ответчиком по 140 делам выступал ПАО «Сбербанк России» (включая подразделения).

Рисунок 2. Ответчики по делам взыскания убытков

При этом большая часть истцов по делам с ПАО «Сбербанк России» являлись физическими лицами. Из общего количества в 31 дело за 2016 год, где истцами выступали юридические лица, ПАО «Сбербанк России» и его подразделения выступили ответчиками в 7 делах.

Средняя сумма иска по рассматриваемым делам в зависимости от типа клиента составляет 9 714 040 рублей для юридических лиц и 421 647 рублей для физических лиц.

Рисунок 3. Средняя сумма иска по типу клиента.

Распределение судебных решений по судам представлено на рисунке 4.

Рисунок 4. Распределение судебных решений по судам

Общая статистика результатов рассмотрения всех дел вне зависимости от типа клиента представлена на рисунке 5.

Рисунок 5. Количество судебных решений за 2016 год.

Таким образом, суды отказывают в удовлетворении иска в 81% случаев.

В случае разделения статистики по типу клиента получаем, что иски клиентов–физических лиц удовлетворяются судами в 24% случаев, а иски клиентов–юридических лиц – почти в 13% случаев.

Рисунок 6. Результаты рассмотрения по искам физических лиц за 2016 год.

Рисунок 7. Результаты рассмотрения
по искам юридических лиц за 2016 год.

Особое внимание необходимо уделить результатам рассмотрения дел, по которым истцами выступали юридические лица.

Иски юридических лиц суды удовлетворяют реже. За 2016 год арбитражные суды вынесли решения по 31 делу, связанным с хищением через ДБО. Общая сумма исков по делам составляет 301 135 239 рублей. Из 31 дела, 27 завершены отказом в удовлетворении иска.

Важно отметить, что из 4 дел, по которым иск был удовлетворен полностью или частично, в 3 случаях суд взыскал деньги не с банковской организации, а с компаний, которые использовались мошенниками для вывода денежных средств. Реальное взыскание с банка имело место только в 1 случае. Однако, в данном деле банк самостоятельно признал свою вину и вернул клиенту сумму похищенных денежных средств. Взыскание по этому делу в размере 32 000 рублей включает в себя проценты за пользование чужими денежными средствами, а также судебные расходы.

Таким образом, за 2016 год нет ни одного решения арбитражного суда, по которому в хищении денежных средств с использованием ДБО была доказана вина банка, и банк по суду был обязан вернуть сумму похищенных денежных средств.

ВЫВОДЫ С УЧЕТОМ ОПЫТА RTM GROUP

В целом негативная практика для клиентов банка обусловлена сложностью доказывания причинно–следственной связи между действиями/бездействием банка и последствиями в виде хищения денежных средств. Если у клиента отсутствуют доказательства прямой вины банка, то решение выносится не в его пользу. Шансы обнаружения доказательств вины банка возрастают в случае возбуждения уголовного дела и качественной работы следствия.

Общими недостатками в ведении дел клиентов являются:

1) Непривлечение экспертов и/или специалистов по информационной безопасности в процесс. Сам факт привлечения специалиста или эксперта в процесс позволяет перевести рассмотрение дела в плоскость выполнения/невыполнения банками существующих требований по информационной безопасности. Такой подход позволяет обнаружить имеющиеся нарушения банком требований законодательства и Банка России, позволяет установить факты наличия уязвимостей системы ДБО. Все это делает возможным исключить из рассмотрения судом части доказательств, которые подтверждают позицию банка и привнести в дело новые доказательства.

2) Отсутствие в делах анализа работы банка в части обеспечения информационной безопасности. Основная часть доказательств по делам хищения через ДБО находится на стороне банка. В случае наличия нарушений со стороны банка, банк не стремится предоставлять информацию о них суду самостоятельно. Поэтому истребование таких доказательств через суд или органы следствия является приоритетной задачей.

3) Изначально ошибочная формулировка позиции и требований. Первое, на что обращает внимание суд – это договоры между банком и клиентом. Попытки оспорить отдельные пункты договора являются бесперспективными. Например, если по условиям договора или какого–то приложения, клиент обязуется использовать средство антивирусной защиты конкретного производителя, то на рабочей станции, с которой осуществляются платежи, должен быть установлен именно такой антивирус. Факт использования средства антивирусной защиты другого производителя нарушает условия договора, как следствие, клиенту будет отказано в иске. Также, любые попытки убедить суд в том, что банк не использует достаточные меры по обеспечению безопасности платежей, будут тщетны, если договор, подписанный клиентом, содержит формулировку о

том, что стороны считают используемые меры по обеспечению безопасности платежей достаточными.

4) Неподача заявления в правоохранительные органы и, как следствие, отсутствие возбужденного уголовного дела. Отсутствие возбужденного уголовного дела по факту хищения денежных средств является крайне серьезной проблемой в доказывании самого факта хищения. Кроме того, возможности следствия в истребовании доказательств несоизмеримо выше, нежели у суда. В настоящий момент, например, существует практика истребования следователями самописных компонентов ДБО в исходных кодах для проведения экспертизы. Результат экспертизы может выявить недостатки и уязвимости в ДБО банка, что повышает шансы доказать вину банка.

5) Неучтенная, негативная для клиентов судебная практика. Настоящее исследование само по себе является доказательством наличия негативной практики для клиента. Клиентам необходимо учитывать данный факт в случае появления возможности выхода на мировое соглашение с банком.

6) Стремление самого клиента провести экспертизу жесткого диска или рабочей станции, с которой осуществлялись платежи. Экспертиза жесткого диска клиента может доказать только вину самого клиента. Факт обнаружения вредоносного программного обеспечения на рабочей станции клиента в момент совершения спорных транзакций является резко негативным обстоятельством для судебного процесса. Даже если экспертиза установит, что вредоносного программного обеспечения нет, это не поможет при доказательстве вины банка.

Анализ содержания кейсов подтверждает, по крайней мере, частичную вину клиента в 80% дел, дошедших до судебного решения. При этом, опыт экспертов RTM Group позволяет сделать вывод о том, что примерно в половине дел имеет место обоюдная вина и клиента, и банка. Вина банка заключается, как минимум, в неисполнении требований Банка России по защите информации и использованию необходимых средств защиты информации. Исполнение указанных требований могло предотвратить хищение. Однако, распространенные в настоящий момент договоры банковского обслуживания перераспределяют риски таким образом, что реально банк не несет ответственности за совершение мошеннических платежей с использованием ДБО даже в тех случаях, когда банк допустил массу критичных нарушений. Авторы настоящего исследования не могут назвать такую практику справедливой. Ведь именно банк является квалифицированным участником рынка, разрабатывает и/или использует системы ДБО, применяет различные системы выявления фальсифицированных транзакций и пр. Таким образом, банк не в меньшей степени, чем клиент, имеет возможность предотвратить хищение. Однако сложившаяся практика не мотивирует банковское сообщество заниматься повышением уровня информационной безопасности своих систем и процессов.

При этом, нельзя утверждать, что банки намеренно пренебрегают вопросами информационной безопасности. За рамки настоящего исследования вынесены кейсы, в которых клиент и банк либо заключили мировое соглашение, либо нашли способ разделить ущерб. Это происходит в тех случаях, когда имеют место грубые нарушения самим банком требований Банка России, законодательства и общих требований по информационной безопасности. В таких случаях банки

предпочитают не доводить дело до суда, даже в тех случаях, когда вероятность победы в суде высока. Таким образом, банки учитывают риски негативных последствий в результате огласки инцидента. В первую очередь это относится к небольшим и региональным банкам.

Если же дело дошло до суда, то положительные судебные решения возможны для клиента только в тех случаях, когда из материалов дела явно следует вина банка, при условии соблюдения клиентом всех возможных условий договора и мер, препятствующих хищению. Например, если клиент уведомил банк о факте компрометации ключей электронной подписи, и данный канал уведомления предусмотрен договором, то в случае хищения денежных средств с использованием указанных ключей уже после обращения клиента, ответственность возлагается на банк. В таких случаях клиент получает полное возмещение ущерба, а также возмещение расходов по судебному разбирательству (экспертиза, работа представителей и т.п.).

RTM GROUP

RTM Group — группа экспертных и юридических компаний, специализирующихся на правовых и нормативно-технических вопросах в области информационных технологий и информационной безопасности.

В RTM Group работает Центр судебных экспертиз, специализирующийся на проведении нормативных и нормативно-технических экспертиз, а также правовое подразделение, осуществляющее сопровождение клиентов, в случае возникновения конфликтов, в том числе судебных, имеющих отношение к информационным технологиям и информационной безопасности.

Компании группы обладают необходимыми лицензиями ФСТЭК России и ФСБ России.

Сотрудники компаний имеют большой опыт экспертной, а также правовой работы и специализируются на проведении следующих видов работ:

- Подготовка судебных и досудебных экспертиз по вопросам информационных технологий, информационной безопасности и защиты информации;
- Приведение деятельности компаний в соответствии с требованиями государственных нормативных актов;
- Экспертиза соответствия требованиям законодательства и требованиям Банка России, ФСТЭК России и ФСБ России;
- Экспертиза в рамках судебных разбирательств, имеющих отношение к вопросам информационных технологий, информационной безопасности и защиты информации. В частности судебно-нормативная экспертиза в делах кражи денежных средств с использованием систем дистанционного банковского обслуживания;
- Экспертиза Технических заданий и Технических проектов на соответствие требованиям договора, законодательства, требованиям регуляторов;
- Участие в судебных процессах, имеющих отношение к вопросам информационных технологий и информационной безопасности;
- Консультационная поддержка юридических подразделений предприятия по вопросам информационной безопасности, включая реакцию на инциденты информационной безопасности, участие во взаимодействии с контрагентами и регуляторами;
- Помощь в разрешении споров, управление потребительскими претензиями, ответные действия на заявления о злоупотреблении данными, содействие в судебных разбирательствах.

Эксперты компании обладают признанными Национальными и Международными сертификациями, такими как CISA, CISM, CISSP, СТО БР ИББС, 27001 и пр.

RTM Group является первым на российском рынке исполнителем судебных нормативно-технических экспертиз в области информационных технологий и информационной безопасности.