

УДК 34

DOI: 10.34670/AR.2024.52.65.038

**Некоторая специфика образования следов
при совершении изготовления, хранения,
перевозки или сбыта поддельных денег
или ценных бумаг (ст. 186 УК РФ),
неправомерного оборота средств
платежей (ст. 187 УК РФ)**

Ефимов Сергей Николаевич

Полковник полиции, адъютант,
Академия управления МВД России,
125993, Российская Федерация, Москва,
ул. Зои и Александра Космодемьянских, 8;
e-mail: aumvd@mvd.ru

Аннотация

Компьютерные следы (электронные, виртуальные, информационные) по своему происхождению относятся к числу наиболее распространенных, запечатлеваемых при совершении таких преступлений, как изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ), совершенных в условиях неочевидности. Что предполагает их поиск, обнаружение, фиксацию, сохранение в процессе расследования вплоть до последующего использования в уголовном судопроизводстве, начиная с момента получения сообщения о преступлении (п. 9 ст. 5 УПК РФ). В данной статье кратко рассматриваются механизм, особенности формирования компьютерных следов, дается их классификация в зависимости от вида преступной деятельности: оборота поддельных денег или ценных бумаг, неправомерного оборота средств платежей (1); непосредственного изготовления указанных объектов, оборота в виде приобретения, сбыта, хранения, транспортировки и перевозки указанных объектов (2); выполнения преступниками факультативных операций, действий, а также использования других вспомогательных технических и иных средств в процессе реализации преступной деятельности (3). Обозначаются активные цифровые следы, при условии если пользователь намеренно делится информацией о себе, делает публикации в социальных сетях или сообщения на сайтах или онлайн-форумах, и пассивные цифровые следы, образующиеся когда информация о пользователе собирается без его непосредственного участия.

Для цитирования в научных исследованиях

Ефимов С.Н. Некоторая специфика образования следов при совершении изготовления, хранения, перевозки или сбыта поддельных денег или ценных бумаг (ст. 186 УК РФ), неправомерного оборота средств платежей (ст. 187 УК РФ) // Вопросы российского и международного права. 2023. Том 13. № 11А. С. 327-334. DOI: 10.34670/AR.2024.52.65.038

Ключевые слова

Компьютерно-технические средства, преступления, следы, поддельные деньги или ценные бумаги, неправомерный оборот средств платежей.

Введение

Компьютерные следы (электронные, виртуальные, информационные) по своему происхождению относятся к числу наиболее распространенных, запечатлеваемых при совершении таких преступлений, как изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ), совершенных в условиях неочевидности. Что предполагает их поиск, обнаружение, фиксацию, сохранение в процессе расследования вплоть до последующего использования в уголовном судопроизводстве, начиная с момента получения сообщения о преступлении (п. 9 ст. 5 УПК РФ). Приведенная зависимость образования следов обуславливается не только штатными компьютерно-техническими средствами (государственными, прошедшими сертификацию), но и теми, которые используют преступники.

Практика показывает, что в зависимости от уровня технической оснащенности и финансовых возможностей преступниками используют и собственные разработки, которые модернизированы или вообще разработаны специально для изготовления поддельных финансовых и иных документов. На это в своих исследованиях обоснованно указывает профессор Ю.В. Гаврилин, раскрывающий содержание в том числе основных цифровых технологий, используемых при подготовке, совершении и сокрытии преступлений [Гаврилин, 2020, 34-45].

Основная часть

Активность в компьютерно-технических средствах и каналах связи между ними предусматривает наличие и сохранение следов. Обусловлено это спецификой предоставления услуг доступа к информационным сетям, которые оказывают определенные провайдеры.

В последнее время в информационно-технической, законодательной, IT-среде и других, близких к данным системам, средах ведется активная дискуссия о правилах хранения учетной информации. Правовыми источниками такой активной дискуссии стало принятие Государственной Думой («Пакет Яровой») ряда законов, которые обязали провайдеров хранить переписку, телефонные звонки и соединения, а также исходящий трафик российских пользователей их услугами. Не вступая в полемику по данному вопросу, лишь отметим, что данный вариант законов основан на принципах обработки и хранения информации в сегменте компьютерно-технического обмена.

Применительно к рассматриваемому нами виду преступлений можно классифицировать компьютерные следы в зависимости от вида преступной деятельности. Во-первых, следы в области оборота поддельных денег или ценных бумаг и неправомерного оборота средств платежей. В данном случае классификация зависит от выбора объекта преступного посягательства: следы в области оборота поддельных денег или ценных бумаг; следы в области оборота средств платежей. Во-вторых, следы непосредственного изготовления указанных объектов и следы, связанные с оборотом в виде приобретения, сбыта, хранения,

транспортировки и перевозки указанных объектов. Здесь основанием классификации следов выступает характер преступной деятельности, еще раз укажем: а) следы непосредственно изготовления поддельных денег, ценных бумаг, средств платежа; б) следы оборота указанных объектов. Их следует именовать основными. В-третьих, смешанные следы при реализации иных вспомогательных действий. Речь идет о всех следах, которые образуются при выполнении факультативных операций преступниками, а также использовании других технических и иных средств в процессе реализации преступной деятельности: следы видео- и фото-фиксации, транспортных средств. Их символически можно назвать факультативными (дополнительными).

Такое деление имеет условный характер, однако позволяет более детально рассмотреть процесс следообразования и возможность его дальнейшего использования в процессе выявления, раскрытия и расследования преступлений в области оборота поддельных денег или ценных бумаг и неправомерного оборота средств платежей. Безусловно, следы в компьютерно-технических средствах и системах являются ключевыми ввиду специфики рассматриваемой преступной деятельности, а также особенностей и возможностей их выявления и фиксации.

Наибольшее значение имеет компьютер лица, участвующего в процессе совершения преступления. Данный объект является носителем как компьютерных, так и традиционных следов. Аналогичное значение как объекта следоносителя имеет средство подвижной сотовой связи (телефон, смартфон, планшет). Существенное значение при расследовании преступлений рассматриваемого вида имеют компьютерные сети, традиционно их разделяют на локальные (Local Area Network), региональные (Metropolitan Area Network) и глобальные (Wide Area Network).

Перечень компьютерных сетей, по мере совершенствования информационных технологий, расширяется, поэтому интерес может представлять, например, персональная сеть, которая функционирует в пределах деятельности разных устройств, принадлежащих одному владельцу. Укажем, что таких сетей при обобщении практики нами не было выявлено. Основной целью выявления компьютерных следов является их принадлежность конкретному лицу для последующей идентификации его как лица, использовавшего компьютерно-техническое средство или сеть в целях совершения преступления. По мнению Ю.В. Гаврилина, к таким относятся следы, «...позволяющих установить лицо, совершившее преступление с использованием информационно-коммуникационных технологии: IP-адрес компьютера в сети, MAC-адрес сетевого оборудования, адрес электронной почты, идентификатор социальной сети, номер банковской карты, произведенные с ней транзакции, номер телефона, информация о соединениях абонента, информация базовых станций мобильной связи, данные систем геолокации и т.п.» [Гаврилин, Шипилов, 2013, 3]. Следственная практика показывает, что приведенные следы характерны и для преступной деятельности, реализуемой в сфере кредитно-денежной системы или иных ценных бумаг, а также иных средств платежа.

Дополнительно еще раз обозначим, что практически весь процесс совершения преступления, связанного со сбытом поддельных денежных средств (после их изготовления, приобретения), осуществляется посредством использования компьютерных сетей. Это относится и к неправомерному обороту средств платежей (распоряжения о переводе денежных средств, документов или средств оплаты), изготовление и передача которых в финансовое учреждение осуществляются преимущественно посредством компьютерно-технических средств, сетей и специальных программ.

Следует назвать еще одну важную составляющую, как бы предопределяющую образование

и выявление следов (и, как результат, последующего установления обстоятельств противоправной деятельности) при совершении преступлений в сфере кредитно-денежной системы или иных ценных бумаг, а также иных средств платежа – установленную и строго регламентированную систему бухгалтерского учета. Как подмечает С.А. Звягин: «...одной из основных защитных функций бухгалтерского учета с позиций теории и практики судебной бухгалтерии является следообразующая, которая означает возможность и способность бухгалтерского учета при взаимодействии с неправомерными действиями и их непосредственном воздействии на учетный процесс образовывать и формировать в собственной информационной среде следы и признаки таких контактов» [Звягин, Фоменко, 2018, 1302-1317].

Дополнительно скажем и о том, что такое положение позитивно, в первую очередь, для формирования следовой картины преступной деятельности, которая находит полное отражение в указанных элементах учета. Во-вторых, наличие качественных знаний о конкретных видах следов и местах их обнаружения в рассматриваемой сфере позволяет достаточно эффективно получать доказательства не только о преступной деятельности, но и о причастности конкретного лица к совершенному преступлению.

Система построения бухгалтерского учета устроена таким образом, что расчетные документы изготавливаются только в двух вариантах: в электронном виде или на бумажном носителе. В обоих случаях документ имеет установленный образец и регламентированную процедуру передачи его в финансовое учреждение. Реализация электронного документооборота осуществляется через систему «Клиент-Банк». Она представляет собой корпоративную информационную систему удаленного банковского обслуживания. Ее составляющими выступает совокупность программно-аппаратных средств, включающая в себя серверную часть (сервер), который располагается на территории банка, и программно-аппаратную часть, находящуюся в компьютерно-технических средствах клиента банка. Данная система согласованно функционирует у клиента и банка посредством телефонной и телекоммуникационной связи¹ [Система «Клиент-Банк», www]. Таким образом, весь процесс от создания документа до его исполнения находит отражение в компьютерно-технических средствах указанной системы. Это в свою очередь является позитивным моментом для обнаружения и изъятия следов преступной деятельности в рассматриваемом формате реализации способа изготовления в целях сбыта средств платежа. При этом, даже в случае реализации усилий по уничтожению следов преступной деятельности, они могут быть реализованы только на компьютерно-технических средствах клиента и только путем уничтожения первичной информации созданного файла в виде расчетного документа. При загрузке в систему «Клиент-Банк» данный документ размещается на сервере банка, где он уже не может быть изменен или модифицирован без разрешения оператора банка, и хранится там в неизменном виде.

Изготовление платежного средства в натуральном бумажном виде вообще предусматривает после его изготовления (что тоже может осуществляться посредством компьютерно-технических средств, имеющихся в распоряжении преступников) необходимость направления в банк. В таком случае данный документ подшивается к номенклатурным делам клиента и

¹ Это автоматизированная компьютерная система электронных расчетов через модемную связь. Данная программа дает возможность одновременно работать с одними и теми же банковскими документами из существенно удаленных друг от друга рабочих мест в любое время суток.

хранится в банке.

Учитывая, что предоставляемые в финансовое учреждение документы должны отвечать определенным требованиям, которые проверяются сотрудником данного учреждения, при их изменении может иметь место интеллектуальный подлог. Если в подлинный документ были внесены сведения, не соответствующие действительности. Но при этом, на начальном этапе реализации способа совершения преступления, данные сведения не могут вызвать подозрение у сотрудников финансового учреждения. Обусловлено это соблюдением всех необходимых требований к рассматриваемым документам.

Как определенный «позитив» следообразования в рассматриваемых нами видах преступной деятельности, нужно указать и на основной источник следовой информации, всегда находящийся в банке, где он не может быть подвержен воздействию заинтересованных лиц. При этом одновременно всегда будет существовать возможность использования его следователем в качестве вещественного доказательства, за исключением случаев активного противодействия со стороны преступной группы. Хотя это обстоятельство в процессе обобщения практики нами не было установлено, но это надо иметь в виду, в том числе и при выдвижении и проверке следственных версий.

Что касается изготовления платежной карты, то эта деятельность предусматривает необходимость наличия технических и программных средств для записи на чип или магнитную ленту платежной карты, которые по сути своей представляют микрокомпьютер, содержащий объем информации о процессах и периодах работы с ней. Сведения, записанные на микропроцессор карты, первично отражаются в программных и операционных средствах компьютерно-технического устройства, используемого для кодировки поддельной платежной карты.

Как отдельную подгруппу компьютерных следов, можно рассматривать результаты, оставляемые пользователями в сетях при подготовке, совершении и сокрытии преступлений, предусмотренных ст. 186, 187 УК РФ. Мы уже обозначали виды сетей и возможные варианты деятельности в них. Следует признать, что сегодня механизм образования информации о лицах, находящихся в сетях, несколько изменился по сравнению с более ранними периодами их функционирования в сети.

Все чаще ученые и специалисты говорят о наличии в сети цифрового следа. Цифровой след, иногда называемый цифровой тенью или электронным следом, – это данные, которые остаются при использовании Интернета. Они включают посещаемые веб-сайты, отправляемые электронные письма и информацию, указываемую в онлайн-формах. Цифровой след можно использовать для отслеживания действий человека и его устройств в Интернете. Пользователи Интернета активно или пассивно создают собственный цифровой след. Применительно к цифровым следам часто используются термины «активный» и «пассивный» [Что такое цифровой след, www].

Пользователь оставляет *активный цифровой след*, когда намеренно делится информацией о себе: делает публикации в социальных сетях или сообщения на сайтах либо онлайн-форумах. Когда пользователь входит на веб-сайт и использует зарегистрированное имя или профиль, все его сообщения будут составлять активный цифровой след. Активный цифровой след остается в процессе заполнения онлайн-форм, например, подписки на информационные рассылки, или при согласии принимать файлы *cookie* в браузере.

Пассивный цифровой след создается, когда информация о пользователе собирается без его

непосредственного участия. Это происходит при сборе на веб-сайте информации о том, сколько раз пользователь посещал сайт, откуда он и его IP-адрес. Это скрытый процесс, о котором граждане могут не догадываться. Другим примером реализации пассивного следа является анализ рекламодателями лайков, репостов и комментариев в социальных сетях с целью последующего профилирования и отображения определенного контента [там же].

Ранее мы обращали внимание на применение возможностей профайлинга. Его информация, в виде цифрового следа, оставленного указанным образом, может использоваться в качестве ориентирующей.

Заключение

В описанных случаях речь идет о сетевых следах, которые оставляют преступники при совершении конкретного преступления. Отметим, что все случаи и варианты выхода в Интернет отражаются на серверах провайдера, там же хранится информация о сайтах и лицах (их электронные адреса), с которыми осуществлялось общение посредством компьютерно-технических средств. Если же в качестве средства совершения преступлений в сфере кредитно-денежной системы или иных ценных бумаг, а также иных средств платежа, использовались локальные сети, например, коммерческой организации, аналогичный комплекс следов будет отражаться на серверах указанного учреждения (время выхода в локальную сеть, адрес зарегистрированного компьютерно-технического средства, а также действия, выполняемые на компьютере).

Обязательным направлением расследования будет являться установление следов нахождения конкретного лица в определенной местности, посредством регистрации его телефона в сети. В настоящее время данная информация активно используется в процессе расследования преступлений как доказательственная. Что касается технологии, то она представляет собой эффективное средство получения информации (производство следственных действий и оперативно-розыскных мероприятий) [Козинкин, 2009]. Одной из проблем установления лиц, причастных к совершению преступлений в сфере кредитно-денежной системы или иных ценных бумаг, а также иных средств платежа, как показывает следственная практика, является обширность киберпространства. Субъекты совершения преступлений могут находиться за пределами Российской Федерации.

Ключевым объектом, наряду с компьютером преступника, содержащим большой объем следов преступной деятельности, является телефон (смартфон, планшет). Сегодня большинство телефонов имеет возможность выхода в любую сеть (телефонную, локальную, глобальную), что порождает возникновение и хранение большого количества следов, по аналогии с компьютерно-техническими средствами, которым в общем виде сегодня является и телефон. Поэтому усиленное внимание следует обращать на все средства, используемые в качестве средств подвижной сотовой связи.

Библиография

1. Гаврилин Ю.В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях. М., 2020. 52 с.
2. Гаврилин Ю.В., Шипилов В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 25. С. 2-5.
3. Звягин С.А., Фоменко Т.Н. Анализ защитных функций бухгалтерского учета и следы правонарушений экономических действий // Экономический анализ: теория и практика. 2018. Т. 17. № 7. С. 1302-1317.

4. Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: автореф. дис. ... канд. юрид. наук. М., 2009. 26 с.
5. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06.07.2016 № 375-ФЗ.
6. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06.07.2016 № 374-ФЗ.
7. О внесении изменений в Федеральный закон «О связи»: Федеральный закон от 02.07.2021 № 319-ФЗ.
8. Положение Банка России от 29.06.2021 № 762-П (ред. от 25.03.2022) «О правилах осуществления перевода денежных средств»: зарегистрировано в Минюсте России 25.08.2021 № 64765.
9. Система «Клиент-Банк». URL: https://www.banki.ru/wikibank/sistema_klient-bank/
10. Стандарт Банка России «Финансовые сообщения в НПС. Обмен финансовыми сообщениями в НПС при переводе денежных средств по инициативе плательщика. Модели связей (СТО БР НПС-2.2-2020)»: принят и введен в действие приказом Банка России от 14.09.2018 № ОД-2400).
11. Что такое цифровой след? URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint>

Some specifics of the formation of traces during the production, storage, transportation or sale of counterfeit money or securities (Article 186 of the Criminal Code of the Russian Federation), illegal circulation of means of payment (Article 187 of the Criminal Code of the Russian Federation)

Sergei N. Efimov

Police Colonel, Adjunct,
Academy of Management of the Ministry of Internal Affairs of Russia,
125993, 8, Zoi i Aleksandra Kosmodem'yanskikh str.,
Moscow, Russian Federation;
e-mail: aumvd@mvd.ru

Abstract

Computer traces (electronic, virtual, information) by their origin are among the most common, captured during the commission of crimes such as the production, storage, transportation or sale of counterfeit money or securities (Article 186 of the Criminal Code of the Russian Federation), illegal circulation of means of payment (Article 187 of the Criminal Code of the Russian Federation), committed in conditions of non-obviousness. Which involves their search, detection, recording, preservation during the investigation process up to subsequent use in criminal proceedings, starting from the moment a report of a crime is received (clause 9 of Article 5 of the Code of Criminal Procedure of the Russian Federation). In the article, the mechanism and features of the formation of computer traces are briefly discussed, their classification is given depending on the type of criminal activity: circulation of counterfeit money or securities, illegal circulation of means of payment (1); direct production of the specified objects, turnover in the form of acquisition, sale, storage, transportation and transportation of the specified objects (2); execution by criminals of optional operations, actions, as well as the use of other auxiliary technical and other means in the process of carrying out criminal activities (3). Active digital traces are designated, provided that the user intentionally shares information about himself, makes publications on social networks or messages on websites or online forums, and passive digital traces, formed when information about the user is collected without his direct participation.

For citation

Efimov S.N. (2023) Nekotoraya spetsifika obrazovaniya sledov pri sovershenii izgotovleniya, khraneniya, perevozki ili sbyta poddel'nykh deneg ili tsennykh bumag (st. 186 UK RF), nepravomernogo oborota sredstv platezhei (st. 187 UK RF) [Some specifics of the formation of traces during the production, storage, transportation or sale of counterfeit money or securities (Article 186 of the Criminal Code of the Russian Federation), illegal circulation of means of payment (Article 187 of the Criminal Code of the Russian Federation)]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (11A), pp. 327-334. DOI: 10.34670/AR.2024.52.65.038

Keywords

Computer hardware, crimes, footprints, counterfeit money or securities, illegal circulation of payment funds.

References

1. *Chto takoe tsifrovoy sled?* [What is a digital footprint?]. Available at: <https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint> [Accessed 11/11/2023]
2. Gavrilin Yu.V. (2020) *O nauchnykh podkhodakh k probleme ispol'zovaniya informatsionno-telekommunikatsionnykh tekhnologii v prestupnykh tselyakh* [On scientific approaches to the problem of using information and telecommunication technologies for criminal purposes]. Moscow.
3. Gavrilin Yu.V., Shipilov V.V. (2013) *Osobennosti sledoobrazovaniya pri sovershenii moshennichestv v sfere komp'yuternoi informatsii* [Features of trace formation when committing fraud in the field of computer information]. *Rossiiskii sledovatel'* [Russian investigator], 25, pp. 2-5.
4. Kozinkin V.A. (2009) *Ispol'zovanie v rassledovanii prestuplenii informatsii, obnaruzhivaemoi v sredstvakh sotovykh sistem podvizhnoi svyazi. Doct. Dis.* [The use of information found in cellular mobile communication systems in the investigation of crimes. Doct. Dis.]. Moscow.
5. *O vnesenii izmenenii v Federal'nyi zakon «O protivodeistvii terrorizmu» i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeistviya terrorizmu i obespecheniya obshchestvennoi bezopasnosti: Federal'nyi zakon ot 06.07.2016 № 374-FZ* [On amendments to the Federal Law “On Countering Terrorism” and certain legislative acts of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public safety: Federal Law No. 374-FZ dated 07/06/2016].
6. *O vnesenii izmenenii v Federal'nyi zakon «O svyazi»: Federal'nyi zakon ot 02.07.2021 № 319-FZ* [On amendments to the Federal Law “On Communications”: Federal Law dated July 2, 2021 No. 319-FZ].
7. *O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeistviya terrorizmu i obespecheniya obshchestvennoi bezopasnosti: Federal'nyi zakon ot 06.07.2016 № 375-FZ* [On amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public safety: Federal Law dated July 6, 2016 No. 375-FZ].
8. *Polozhenie Banka Rossii ot 29.06.2021 № 762-P (red. ot 25.03.2022) «O pravilakh osushchestvleniya perevoda denezhnykh sredstv»: zaregistrirvano v Minyuste Rossii 25.08.2021 № 64765* [Bank of Russia Regulation No. 762-P dated June 29, 2021 (as amended on March 25, 2022) “On the rules for transferring funds”: registered with the Ministry of Justice of Russia on August 25, 2021 No. 64765].
9. *Sistema «Klient-Bank»* [“Client-Bank” system]. Available at: https://www.banki.ru/wikibank/sistema_klient-bank/ [Accessed 11/11/2023]
10. *Standart Banka Rossii «Finansovye soobshcheniya v NPS. Obmen finansovymi soobshcheniyami v NPS pri perevode denezhnykh sredstv po initiative platel'shchika. Modeli svyazei (STO BR NPS-2.2-2020)»: prinyat i vveden v deistvie prikazom Banka Rossii ot 14.09.2018 № OD-2400* [Bank of Russia standard “Financial messages in NPS. Exchange of financial messages in the NPS when transferring funds at the initiative of the payer. Models of connections (STO BR NPS-2.2-2020)”: adopted and put into effect by Order of the Bank of Russia dated September 14, 2018 No. OD-2400].
11. Zvyagin S.A., Fomenko T.N. (2018) *Analiz zashchitnykh funktsii bukhgalterskogo ucheta i sledy nepravomernykh ekonomicheskikh deistvii* [Analysis of the protective functions of accounting and traces of illegal economic actions]. *Ekonomicheskii analiz: teoriya i praktika* [Economic analysis: theory and practice], 17, 7, pp. 1302-1317.