IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
LUFKIN DIVISION

SECURE MOBILE TRANSACTIONS LLC, Plaintiff, v. BANK OF TEXAS, A DIVISION OF BOFK, N.A., Defendant.	CIVIL ACTION NO. 9:25-cv-115 **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Secure Mobile Transactions LLC ("Secure Mobile" or "Plaintiff") files this original complaint against Defendant Bank of Texas, a Division of BOFK, N.A. ("Bank of Texas"), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Secure Mobile is a limited liability company formed under the laws of the State of Texas, with a place of business at 2323 Oak Alley, Tyler, Texas.

2. Bank of Texas, a Division of BOFK, N.A. is a company duly organized and existing under the laws of Texas and has a place of business in McKinney, Texas including, for example, 1500 N Central Expressway, McKinney, Texas 75070. Bank of Texas, a Division of BOFK, N.A., may also be served with process through its registered agent, CT Corporation System at 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

3. Bank of Texas and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country's largest banking and financial service entities, including under the Bank of Texas brand.

4. Bank of Texas and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Bank of Texas and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Bank of Texas and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Bank of Texas and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

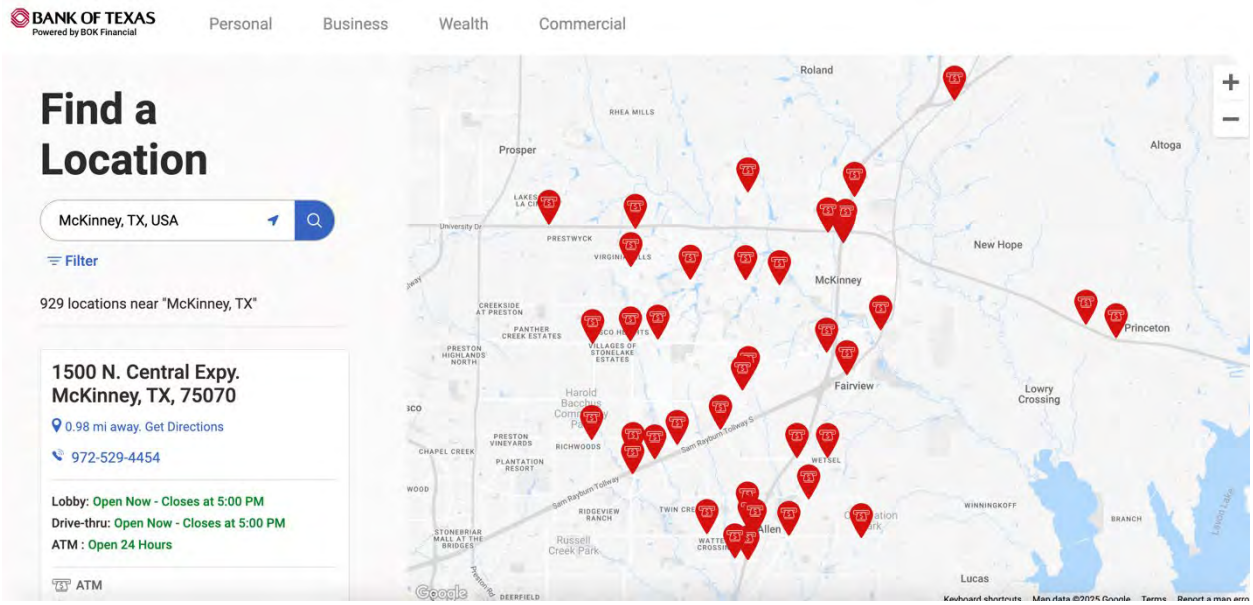
JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Bank of Texas pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Bank of Texas has done and continues to do business in Texas; and (ii) Bank of Texas has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations,

inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Bank of Texas has committed and continues to commit acts of patent infringement in this district. For example, Bank of Texas cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Bank of Texas induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Bank of Texas has regular and established places of business in this district, including at least at 1500 North Central Expy, McKinney, Texas, and at numerous other locations:



(Source: https://locations.bankoftexas.com/search?q=33.1983388%2C-96.6389342&qp=McKinney%2C%20TX%2C%20USA&l=en).

(Source: screenshot from Google Maps Street View).

THE TECHNOLOGY

11. The patents-in-suit generally pertain to methods of enabling point-of-sale terminals to execute transactions associated with smartphones without having to transmit financial account numbers to the point-of-sale terminals. The technology disclosed by the patents was developed by Michael Craft, a project manager with over 20 years of experience in the payment and payment system technology space. Mr. Craft is listed as an inventor on nine U.S. patents. Secure Mobile's patents (or the applications leading to them) have been cited during patent prosecution hundreds of times, including by numerous leading companies in the payment authorization industry such as Capital One, JP Morgan, First Data, and Mastercard.

12. The patents-in-suit, U.S. Patent Nos 9,792,596; 10,546,285; and 11,288,647 (collectively, the "Asserted Patents"), teach systems, including payment processing systems, for securely and effectively enabling mobile phone based transactions at a point of sale terminal. Through the specific use of servers, point of sale terminals, and mobile devices these systems act to reduce credit card and/or debit card fraud and misuse through their use virtual account IDs and transaction-specific unique codes. The technology in the Asserted Patents improves the

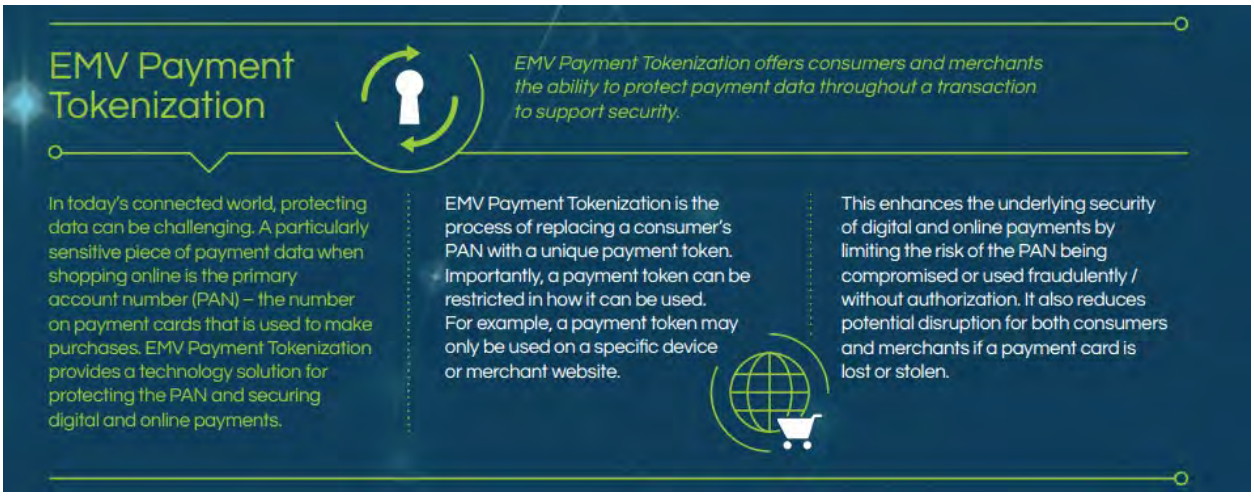
underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

13. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have lead to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall's, was hit with a cyber attack that resulted in the theft of credit cards leading to over $100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

14. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as "a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment" and as "enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs." (Source: https://www.emvco.com/emv-technologies/payment-tokenisation/).

15. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

16. Indeed, as recently as February of 2021, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents "provides a technology solution for protecting the PAN and securing digital and online payments":



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

17. That same EMVCo document notes that "In today's connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases" and that EMVCo's payment tokenization "enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization." The document also states that the "Payment Tokenisation Specification provides an interoperable Technical Framework." (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

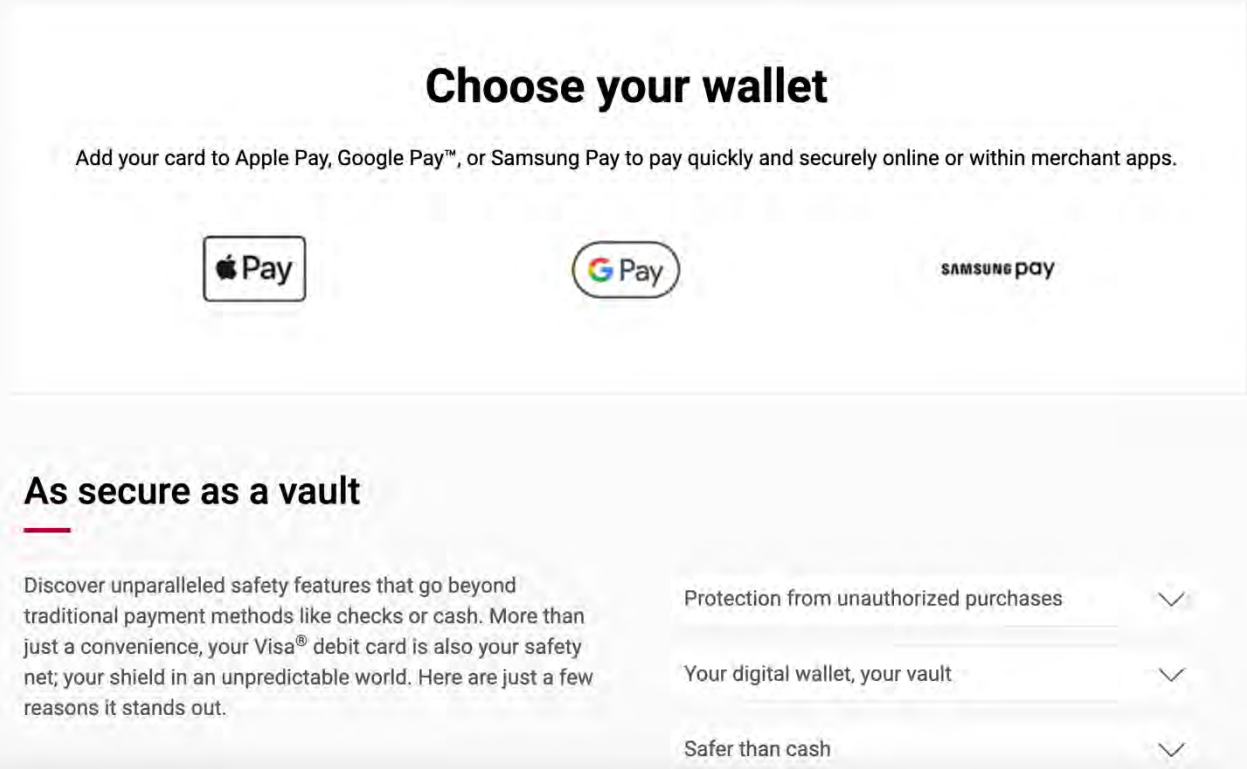
COUNT I

INFRINGEMENT OF U.S. PATENT NO. 9,792,596

18. On October 17, 2017, United States Patent No. 9,792,596 ("the 596 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Mobile Phone Based Rebate Device for Redemption at a Point of Sale Terminal."

19. Secure Mobile is the owner of the 596 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 596 Patent against infringers, and to collect damages for all relevant times.

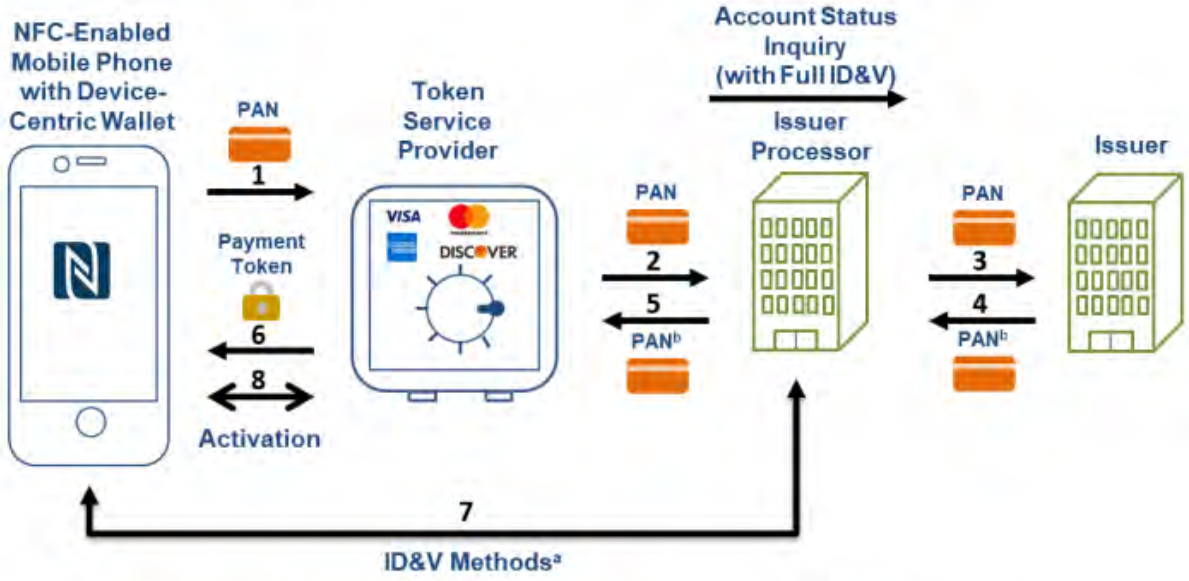
20. Bank of Texas offers debit and/or credit cards, such as the Bank of Texas Visa Debit Card, that are used with an authentication system that authenticates the identity of a Bank of Texas card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). The Bank of Texas card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



(Source: https://www.bankoftexas.com/personal/products-and-services/personal-banking/account-services/online-and-mobile-banking/digital-wallets).

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

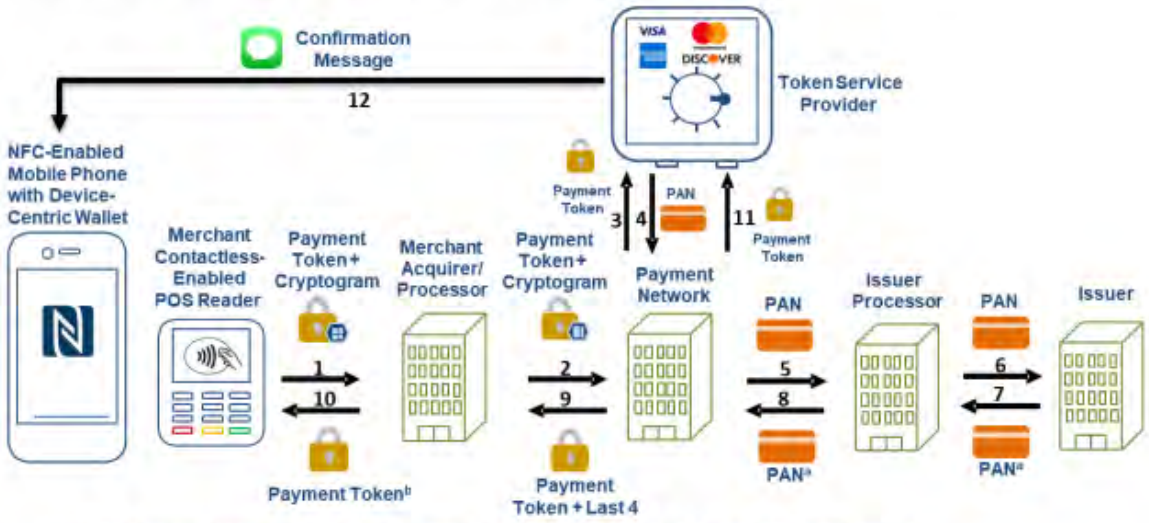
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

21. The Accused Instrumentality includes a method of enabling a physical point of sale (POS) terminal to execute a transaction associated with an Internet capable mobile device to completion without said physical point of sale (POS) terminal ever having received a financial account number from said Internet capable mobile device. For example, a NFC (near field communication) merchant terminal that takes a Bank of Texas debit or credit card that is stored on a user's mobile device executes a transaction without ever having received the actual account number from the phone. A Bank of Texas account holder requests Bank of Texas to provision a

specific Bank of Texas debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Bank of Texas card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. In summary, the terminal is given a payment token by the mobile device that does not include the financial account number.

22. Moreover, Plaintiff alleges that each of element of at least Claim 1 are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

23. Defendants thus infringe one or more claims of the 596 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 596 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 596 Patent.

24. Bank of Texas has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 596 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

25. Bank of Texas has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 596 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 596 Patent by others and Bank of Texas will continue to do so unless enjoined by this Court. Bank of Texas's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 596 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Bank of Texas knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 596 Patent.

26. Bank of Texas continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 596 Patent.

27. Bank of Texas has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 596 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 596 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

28. Bank of Texas has committed these acts of infringement without license or authorization.

29. By engaging in the conduct described herein, Bank of Texas has caused injury to Secure Mobile and Secure Mobile has been damaged and continues to be damaged as result thereof and Bank of Texas is thus liable to Secure Mobile for infringement of the 596 Patent, pursuant to 35 U.S.C. § 271.

30. As a direct and proximate result of Bank of Texas's infringement of the 596 Patent, Secure Mobile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Secure Mobile for Bank of Texas's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

31. In addition, the infringing acts and practices of Bank of Texas have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause

immediate and irreparable harm and damage to Secure Mobile for which there is no adequate remedy at law, and for which Bank of Texas is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Secure Mobile is entitled to compensation for any continuing and/or future infringement up until the date that Bank of Texas is finally and permanently enjoined from further infringement.

32. Bank of Texas has had actual knowledge of the 596 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Bank of Texas will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 596 Patent.

33. Bank of Texas has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 596 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

34. Secure Mobile has been damaged as a result of the infringing conduct by Bank of Texas alleged above. Thus, Bank of Texas is liable to Secure Mobile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

35. Secure Mobile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 596 Patent.

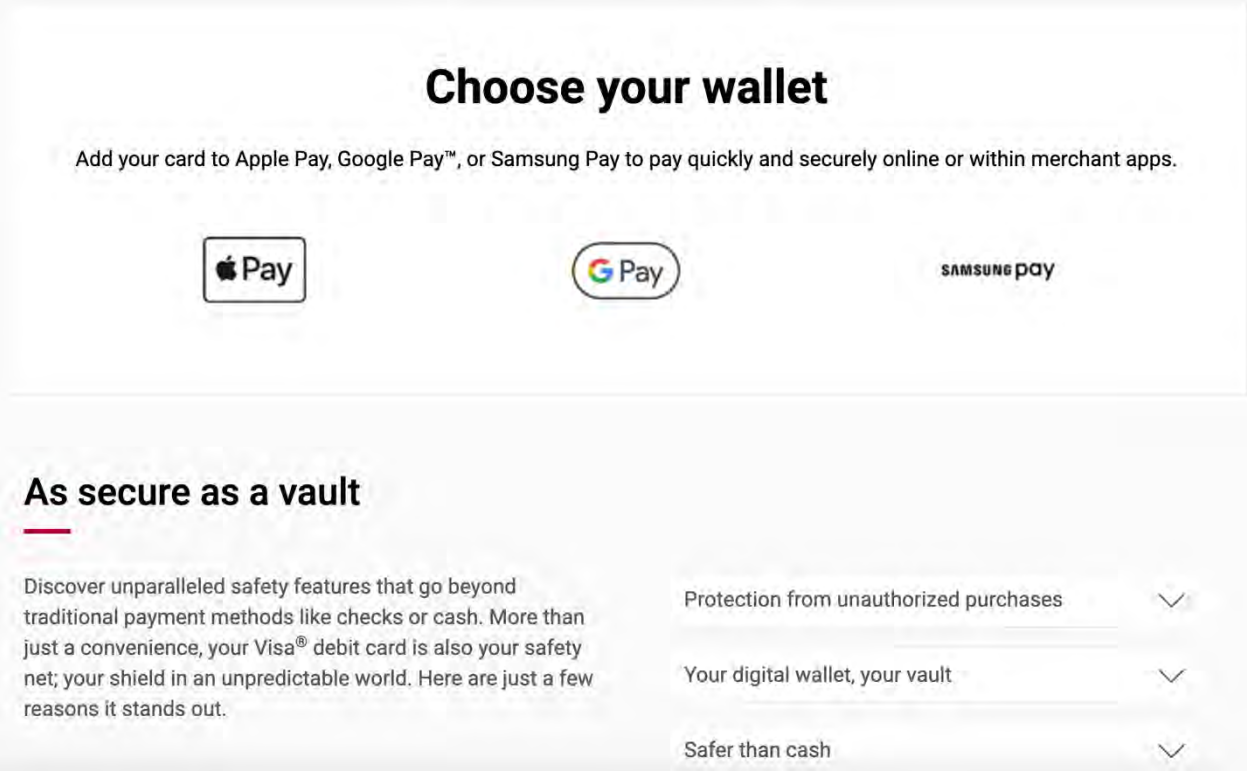
COUNT II

INFRINGEMENT OF U.S. PATENT NO. 10,546,285

36. On January 20, 2020, United States Patent No. 10,546,285 ("the 285 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Mobile Phone Based Transactions at a Point of Sale Terminal."

37. Secure Mobile is the owner of the 285 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 285 Patent against infringers, and to collect damages for all relevant times.

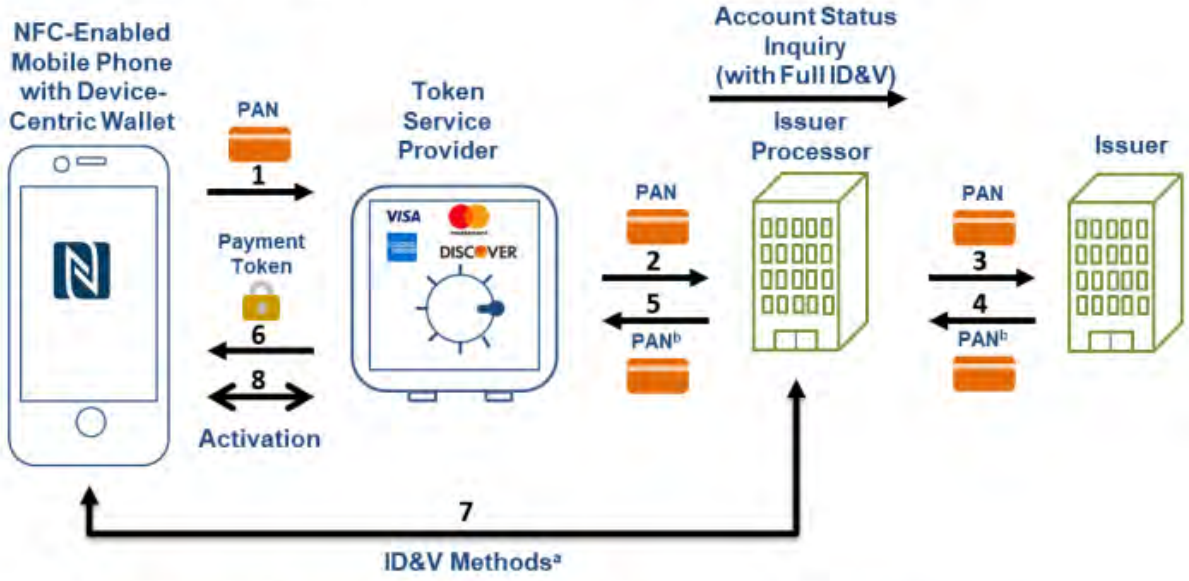
38. Bank of Texas offers debit and/or credit cards, such as the Bank of Texas Visa Debit Card, that are used with an authentication system that authenticates the identity of a Bank of Texas card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). The Bank of Texas card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



(Source: https://www.bankoftexas.com/personal/products-and-services/personal-banking/account-services/online-and-mobile-banking/digital-wallets).

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

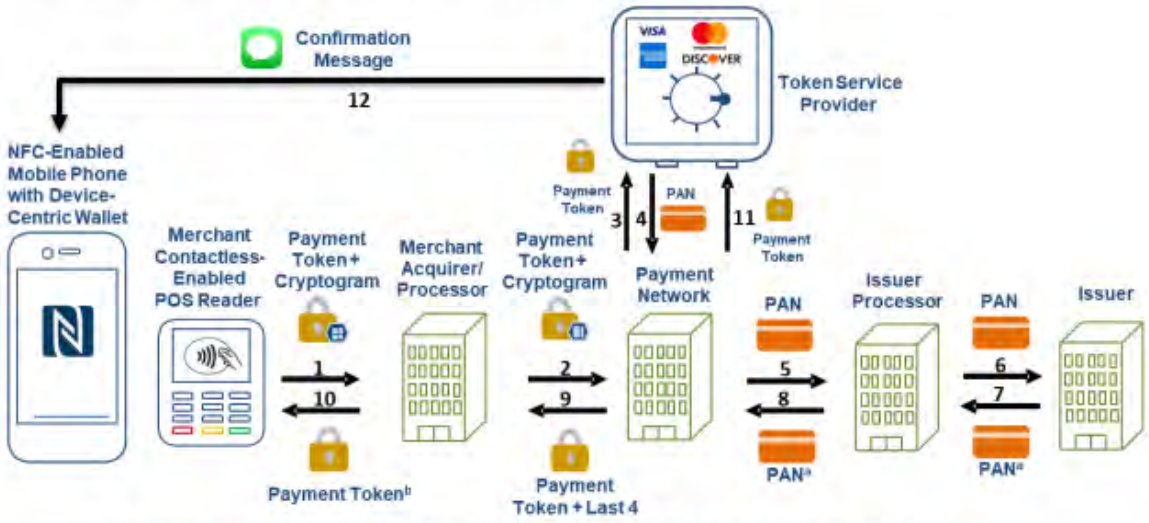
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

39. The Accused Instrumentality includes a method of enabling a physical point of sale terminal to execute a transaction associated with an Internet capable mobile device to completion without said physical point of sale terminal ever having received a financial account number from said Internet capable mobile device. For example, a NFC (near field communication) merchant terminal that takes a Bank of Texas debit or credit card that is stored on a user's mobile device executes a transaction without ever having received the actual account number from the phone. A Bank of Texas account holder requests Bank of Texas to provision a specific Bank of

Texas debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Bank of Texas card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. In summary, the terminal is given a payment token by the mobile device that does not include the financial account number.

40. Moreover, Plaintiff alleges that each of element of at least Claim 7 are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

41. Defendants thus infringe one or more claims of the 285 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 7 of the 285 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 285 Patent.

42. Bank of Texas has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 7 of the 285 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

43. Bank of Texas has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 7 of the 285 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 285 Patent by others and Bank of Texas will continue to do so unless enjoined by this Court. Bank of Texas's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 285 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Bank of Texas knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 285 Patent.

44. Bank of Texas continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 285 Patent.

45. Bank of Texas has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 7 of the 285 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 285 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

46. Bank of Texas has committed these acts of infringement without license or authorization.

47. By engaging in the conduct described herein, Bank of Texas has caused injury to Secure Mobile and Secure Mobile has been damaged and continues to be damaged as result thereof and Bank of Texas is thus liable to Secure Mobile for infringement of the 285 Patent, pursuant to 35 U.S.C. § 271.

48. As a direct and proximate result of Bank of Texas's infringement of the 285 Patent, Secure Mobile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Secure Mobile for Bank of Texas's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

49. In addition, the infringing acts and practices of Bank of Texas have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Secure Mobile for which there is no adequate remedy at

law, and for which Bank of Texas is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Secure Mobile is entitled to compensation for any continuing and/or future infringement up until the date that Bank of Texas is finally and permanently enjoined from further infringement.

50. Bank of Texas has had actual knowledge of the 285 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Bank of Texas will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 285 Patent.

51. Bank of Texas has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 285 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

52. Secure Mobile has been damaged as a result of the infringing conduct by Bank of Texas alleged above. Thus, Bank of Texas is liable to Secure Mobile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

53. Secure Mobile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 285 Patent.

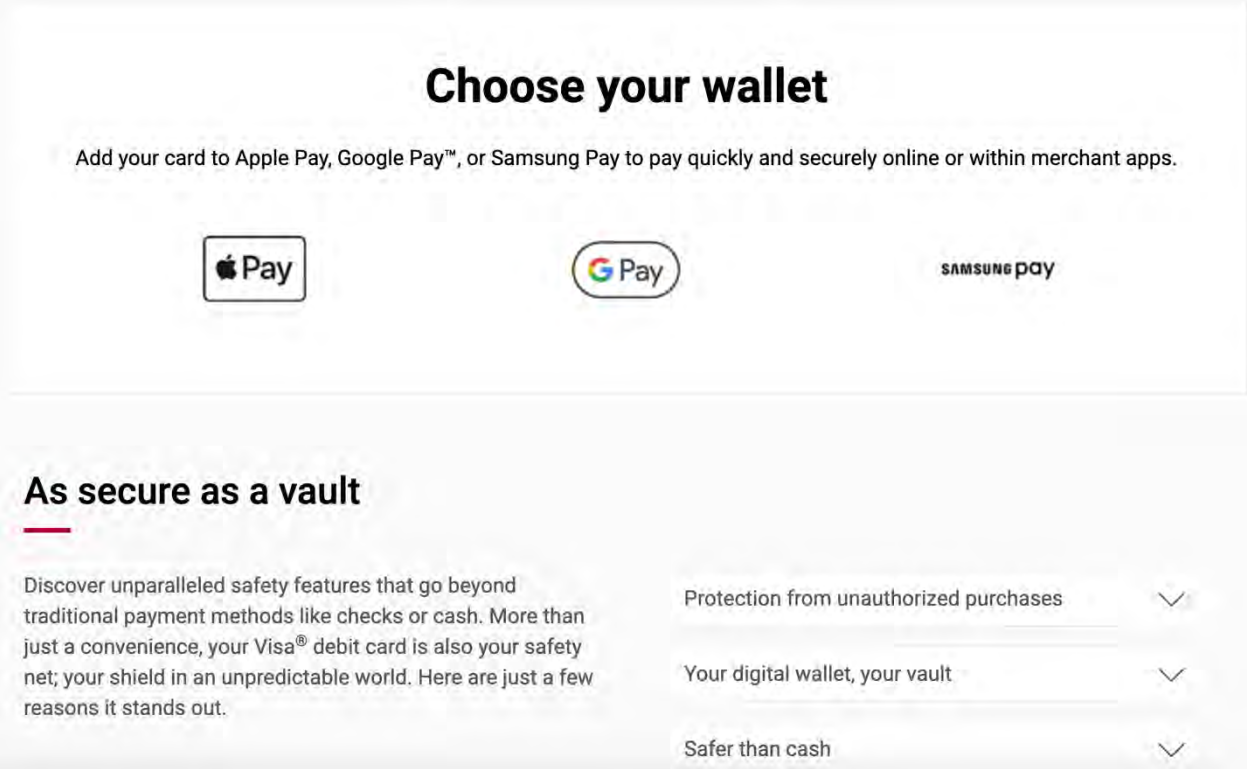
COUNT III

INFRINGEMENT OF U.S. PATENT NO. 11,288,647

54. On March 29, 2022, United States Patent No. 11,288,647 ("the 647 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Radio Device Based Transaction at a Point of Sale Terminal."

55. Secure Mobile is the owner of the 647 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 647 Patent against infringers, and to collect damages for all relevant times.

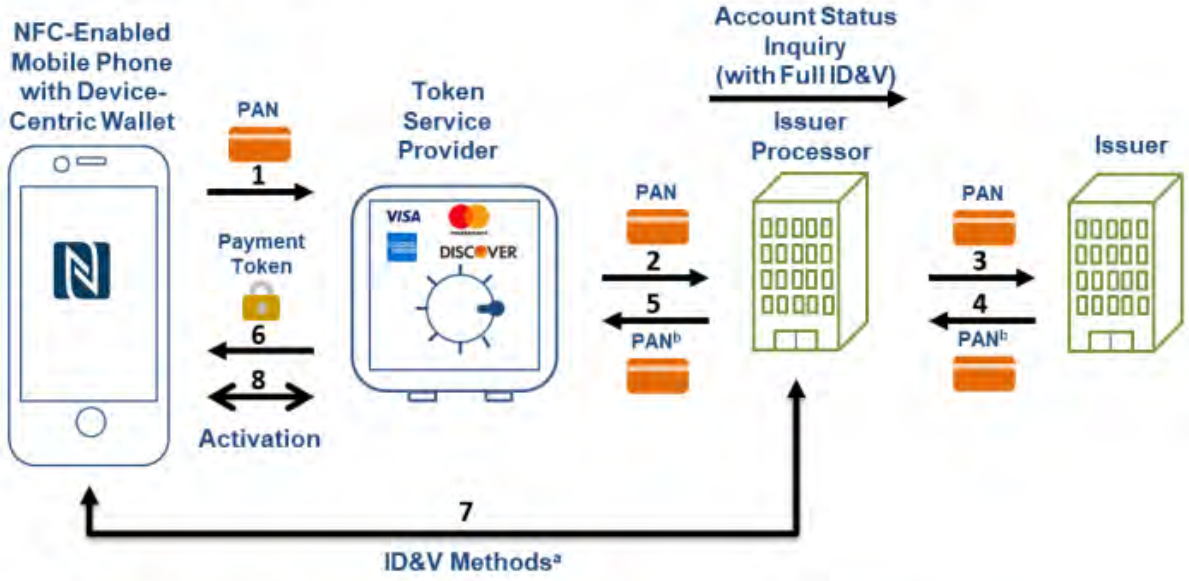
56. Bank of Texas offers debit and/or credit cards, such as the Bank of Texas Visa Debit Card, that are used with an authentication system that authenticates the identity of a Bank of Texas card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). The Bank of Texas card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



(Source: https://www.bankoftexas.com/personal/products-and-services/personal-banking/account-services/online-and-mobile-banking/digital-wallets).

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

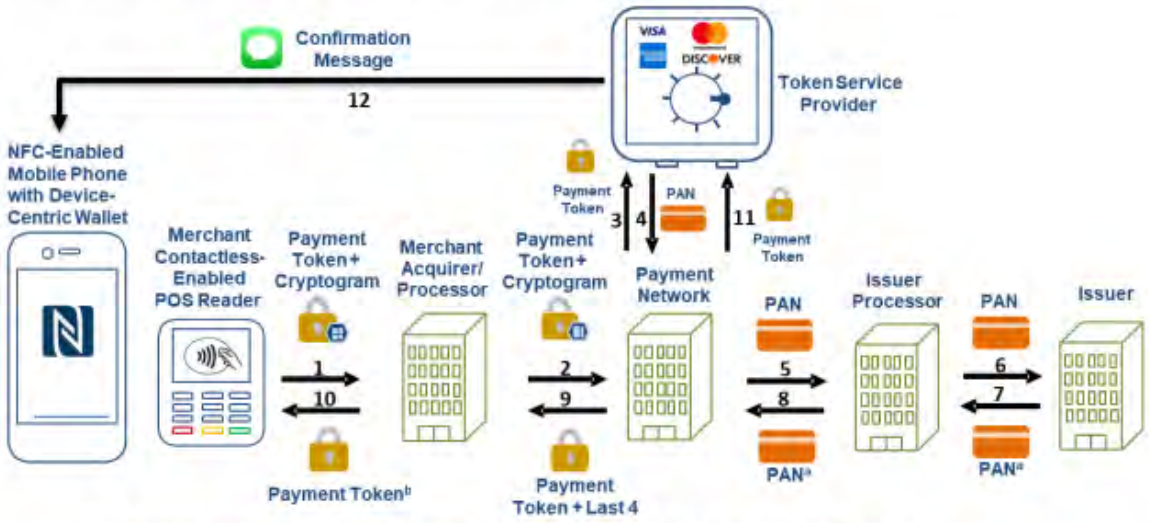


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

57. The Accused Instrumentality includes a method performed by a physical point of sale system to execute a transaction associated with a radio device to completion without the physical point of sale system ever having received a financial account number from the radio device. For example, a NFC (near field communication) merchant terminal that takes a Bank of Texas debit or credit card that is stored on a user's mobile device executes a transaction without ever having received the actual account number from the phone. A Bank of Texas account holder requests Bank of Texas to provision a specific Bank of Texas debit and/or credit card for use on his or her

mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Bank of Texas card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. In summary, the terminal is given a payment token by the mobile device that does not include the financial account number.

58. Moreover, Plaintiff alleges that each of element of at least Claim 7 are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

59. Defendants thus infringe one or more claims of the 647 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 7 of the 647 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 647 Patent.

60. Bank of Texas has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 7 of the 647 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

61. Bank of Texas has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 7 of the 647 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 647 Patent by others and Bank of Texas will continue to do so unless enjoined by this Court. Bank of Texas's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 647 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Bank of Texas knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 647 Patent.

62. Bank of Texas continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 647 Patent.

63. Bank of Texas has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 7 of the 647 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 647 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

64. Bank of Texas has committed these acts of infringement without license or authorization.

65. By engaging in the conduct described herein, Bank of Texas has caused injury to Secure Mobile and Secure Mobile has been damaged and continues to be damaged as result thereof and Bank of Texas is thus liable to Secure Mobile for infringement of the 647 Patent, pursuant to 35 U.S.C. § 271.

66. As a direct and proximate result of Bank of Texas's infringement of the 647 Patent, Secure Mobile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Secure Mobile for Bank of Texas's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

67. In addition, the infringing acts and practices of Bank of Texas have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Secure Mobile for which there is no adequate remedy at

law, and for which Bank of Texas is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Secure Mobile is entitled to compensation for any continuing and/or future infringement up until the date that Bank of Texas is finally and permanently enjoined from further infringement.

68. Bank of Texas has had actual knowledge of the 647 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Bank of Texas will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 647 Patent.

69. Bank of Texas has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 647 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

70. Secure Mobile has been damaged as a result of the infringing conduct by Bank of Texas alleged above. Thus, Bank of Texas is liable to Secure Mobile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

71. Secure Mobile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 647 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

72. Bank of Texas has also indirectly infringed the 596 Patent, the 285 Patent, and the 647 Patent by inducing others to directly infringe the 596 Patent, the 285 Patent, and the 647 Patent. Bank of Texas has induced the end-users, Bank of Texas's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 596 Patent, the 285 Patent, and the 647 Patent by using the Accused Instrumentality.

73. Bank of Texas took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 596 Patent, Claim 7 of the 285 Patent, and Claim 7 of the 647 Patent.

74. Such steps by Bank of Texas included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

75. Bank of Texas has performed these steps, which constitute induced infringement, with the knowledge of the 596 Patent, the 285 Patent, and the 647 Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

76. Bank of Texas was and is aware that the normal and customary use of the Accused Instrumentality by Bank of Texas's customers would infringe the 596 Patent, the 285 Patent, and the 647 Patent. Bank of Texas's inducement is ongoing.

77. Bank of Texas directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

78. Bank of Texas took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 596 Patent, Claim 7 of the 285 Patent, and Claim 7 of the 647 Patent.

79. Bank of Texas performed these steps, which constitute induced infringement, with the knowledge of the 596 Patent, the 285 Patent, and the 647 Patent and with the knowledge that the induced acts would constitute infringement.

80. Bank of Texas's inducement is ongoing.

81. Bank of Texas has also indirectly infringed by contributing to the infringement of the 596 Patent, the 285 Patent, and the 647 Patent. Bank of Texas has contributed to the direct infringement of the 596 Patent, the 285 Patent, and the 647 Patent by the end-user of the Accused Instrumentality.

82. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 596 Patent, the 285 Patent, and the 647 Patent, including, for example, at least Claim 1 of the 596 Patent, Claim 7 of the 285 Patent, and Claim 7 of the 647 Patent.

83. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 596 Patent, the 285 Patent, and the 647 Patent.

84. The special features constitute a material part of the invention of one or more of the claims of the 596 Patent, the 285 Patent, and the 647 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

85. Bank of Texas's contributory infringement is ongoing.

86. Bank of Texas's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Bank of Texas, at least since the filing of the Complaint.

87. Bank of Texas has had knowledge of the 596 Patent, the 285 Patent, and the 647 Patent at least since the filing of the Complaint.

88. Bank of Texas's customers have infringed the 596 Patent, the 285 Patent, and the 647 Patent.

89. Bank of Texas encouraged its customers' infringement.

90. Bank of Texas's direct and indirect infringement of the 596 Patent, the 285 Patent, and the 647 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Secure Mobile's rights under the patents.

91. Secure Mobile has been damaged as a result of the infringing conduct by Bank of Texas alleged above. Thus, Bank of Texas is liable to Secure Mobile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Secure Mobile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Secure Mobile requests that the Court find in its favor and against Bank of Texas, and that the Court grant Secure Mobile the following relief:

a. Judgment that one or more claims of the 596 Patent, the 285 Patent, and the 647 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Bank of Texas and/or all others acting in concert therewith;

b. A permanent injunction enjoining Bank of Texas and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 596 Patent, the 285 Patent, and the 647

Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 596 Patent, the 285 Patent, and the 647 Patent by such entities;

c. Judgment that Bank of Texas account for and pay to Secure Mobile all damages to and costs incurred by Secure Mobile because of Bank of Texas's infringing activities and other conduct complained of herein, including an award of all increased damages to which Secure Mobile is entitled under 35 U.S.C. § 284;

d. That Secure Mobile be granted pre-judgment and post-judgment interest on the damages caused by Bank of Texas's infringing activities and other conduct complained of herein;

e. That this Court declare this an exceptional case and award Secure Mobile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Secure Mobile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: April 8, 2025

Respectfully submitted,

/s/ *Matthew J. Antonelli*
Matthew J. Antonelli
Texas Bar No. 24068432
matt@ahtlawfirm.com
Zachariah S. Harrington
Texas Bar No. 24057886
zac@ahtlawfirm.com
Larry D. Thompson, Jr.
Texas Bar No. 24051428
larry@ahtlawfirm.com
Rehan M Safiullah
Texas Bar No. 24066017
rehan@ahtlawfirm.com
Hannah D. Price

Texas Bar No. 24116921
hannah@ahtlawfirm.com
ANTONELLI, HARRINGTON
& THOMPSON LLP
4306 Yoakum Blvd., Ste. 450
Houston, TX 77006
(713) 581-3000

Stafford Davis
State Bar No. 24054605
sdavis@stafforddavisfirm.com
Catherine Bartles
Texas Bar No. 24104849
cbartles@stafforddavisfirm.com
THE STAFFORD DAVIS FIRM
815 South Broadway Avenue
Tyler, Texas 75701
(903) 593-7000
(903) 705-7369 fax

Attorneys for Secure Mobile Transactions LLC