Combining Ubiquity with Security

for 2-Way Mobile Banking and Payments

ClairMail®

ClairMail Security White Paper – June 2008

Introduction

Financial institutions (FIs) face a dilemma: increasingly, mobile customers are demanding mobile access to their accounts. However, there are currently no end-to-end security standards for mobile communications. Further, customer confidence in electronic commerce in general is unsteady, given well-publicized security threats related to online fraud and identity theft.

In its recent Mobile Banking Security study, Javelin Strategy & Research reports that 33% of consumers perceived mobile banking as "too risky" and 34% were undecided in terms of how they felt toward the channel. Given the nascent stage of mobile banking, it is not surprising that consumers would be uncertain or wary. Looking back at online banking trends in 2003, Javelin data shows that 46% of consumers avoided online banking. The good news is that number has now dropped to 21% in 2007.

In order to realize similar customer acceptance for mobile banking, FIs must seek a solution that not only solves security concerns, it must also be simple to use and easy to deploy to all customers. FIs must bear these fundamental objectives in mind when weighing the various options for mobile banking, all of which have very different security and usage paradigms.

The innovative ClairMail System (see below) is the industry's first offering to strike the appropriate balance between solid security, universal availability and ease of use. The ClairMail System is the only platform capable of supporting — and securing — the three modes available on virtually all mobile phones, including text messaging (SMS), mobile browsers and client applications. Moreover, only ClairMail provides a secure mobile banking and payments solution for 2-way customer interaction on any mobile phone – regardless of manufacturer, model or carrier. It protects the privacy and integrity of mobile transactions while making the service both intuitive and ubiquitous.

This white paper introduces the three basic alternatives FIs have for offering mobile banking, and describes how the multiple layers of security in the ClairMail System combine to guard against all security threats and create a trusted path between mobile customers and their account information. The subject matter is of particular interest to executive-level management, security personnel and IT decision-makers.

ClairMail System

The ClairMail System optimizes any mobile phone for 2-way customer interaction—with no new mobile phone software required. Using any phone's existing software and standard capabilities, the ClairMail System's breakthrough platform and applications enable FIs to provide a comprehensive suite of convenient, secure and on-demand services to their customers. With the ClairMail System, FIs can give customers direct access to their private account information, and simultaneously directly access their customers using the same system. No other solution in the market matches the 2-way customer interaction capabilities of the ClairMail System.

The ClairMail System is:

- *Download-free* – No downloading of new mobile phone software is needed, because it leverages software already installed on mobile phones.
- *Device Agnostic* – Works with any mobile phone, regardless of manufacturer, model, operating system or carrier.
- *Standards-based* – Utilizes standards-based technologies on the ClairMail System platform, which can reside on-premise behind the firewall or in a highly secure managed service environment.
- *Intuitive* – Uses existing functionality that customers are already familiar with and comfortable using.
- *Secure* – Meets and exceeds FFIEC's stringent requirements for multifactor authentication.
- *Rapidly Deployed* – Delivers the fastest time to value.
- *Cost-effective* – Reduces costs in other customer interaction channels—particularly IVR and call centers—effectively paying for itself in just a few months.

ClairMail®

The Inevitability of Mobility

Numerous analysts are providing extremely optimistic projections for the future of mobile banking. TowerGroup forecasts that more than 40 million U.S. consumers will be using mobile banking by 2012. Celent projects in its *U.S. Mobile Banking: Beyond the Buzz* study that 30% of all online banking households will engage in mobile banking by the end of 2010. Clearly, the prospects for mobile banking are quite promising.

Research indicates strong consumer demand for mobile banking today. Celent reports that 73% of consumers want to see account balance information on mobile phones and 53% want transaction history; half of 18-25 year-olds said that the availability of mobile banking is an important factor in selecting a financial institution. Javelin Strategy and Research reports that 48% of consumers would view more eBills if alerts were sent to their mobile phones and 45% indicated that receiving unusual account activity alerts would be of value.

Despite this clear interest and opportunity, security concerns have prevented some FIs from taking full advantage of their customers' mobile communications capabilities. There are perceived risks with mobility, especially with most mobile phones lacking the personal firewall, anti-virus software and other protections common today on PCs. As such, mobile phones can be vulnerable to a variety of threats depending upon which approach is taken—including spoofing, phishing, vishing, man-in-the-middle attacks, SMiShing, malware and others (see Glossary of Potential Threats).

But these threats can now all be effectively mitigated by selecting an approach that fully adheres to fundamental tenets of solid security measures and by actively and seamlessly involving the customer in verifying the legitimacy of transactions.

Mobile Banking Options

To meet the increasing demand for mobile banking, some FIs are beginning to deploy solutions. Three fundamental options exist:

1. Mobile browsers
2. Client applications
3. Existing phone software (e.g. SMS)

These approaches differ substantially in how they satisfy the business requirements of a successful—and secure—mobile access solution.

Glossary of Potential Threats

Cloning – Copying the identity of one mobile phone to another, allowing the perpetrator to masquerade as the victim, normally with the intent to have calls and other services billed to the victim's cellular account.
Hijacking – A type of network security attack in which the attacker takes control of a communication between two entities, masquerading as one of them.
Malicious Code – Software in the form of a virus, worm, or other "malware" intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity or availability of an information system.
Malware – A contraction for "malicious software" (see *Malicious Code*) that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system, or otherwise annoying or disrupting the victim.
Man-in-the-middle Attack – An attack on the authentication protocol exchange in which the attacker positions himself between the claimant and verifier with the intent to intercept and alter data traveling between them.
Phishing – Tricking a victim into disclosing sensitive personal information or downloading malware through an email.
Redirecting – Intercepting a communication by substituting a fraudulent address or identity, potentially by using a Man-in-the-Middle attack.
SMiShing – A contraction of "SMS phishing" (see *Phishing*) targeting the Short Message Service on mobile phones.
Spoofing – Sending a network packet that appears to come from a legitimate source, rather than its actual source.
Vishing – A contraction of "voice and phishing" (see *Phishing*), in which victims are tricked into disclosing sensitive personal information through a phone call.

Mobile Browsers

With the growing popularity of online banking, the use of mobile browsers for mobile banking seems to be a natural fit. In its recent mobile banking report, Javelin highlights numerous strengths of mobile browsers for this purpose, including a) no need for customers to download software, b) better browser capabilities from mobile network improvements, c) automatic updates for consumers, and d) familiarity of experience (similar to online banking experience).

Despite these strengths, mobile browsers also come with numerous problems:

a) Form factor: Mobile browsers are inhibited by the small screen and the number of clicks that are often required to complete a task. Trying to make a tiny Web page both visible and easily navigable requires completely rewriting existing Web applications designed for the ample real estate on PC screens. Plus, the customer experience may suffer with lag times and dropped connections.

b) Limited availability: Smartphones and PDAs compose less than 10% of the phones in use, and are sold at about that same rate. Additionally, many mobile phones lack mobile browsers, and not all users with Web/WAP-enabled phones have signed up for the more costly broadband data plans required.

c) Vulnerability to attacks: Mobile phones lack the personal firewalls, anti-virus software and other protections common on PCs, so mobile browsers are susceptible to threats such as phishing, malware and man-in-the-middle attacks. Additionally, it is likely that all implemented protection mechanisms take place in the same session to the mobile device, never going out-of-band or crossing protocols. This is due to the synchronous mobile browser user interface and modality issues; in other words, going “out-of-band,” would require a user to close the browser session and switch to another application (e.g. voice or SMS).

d) Cost factors: Data plan costs can be high with the current mobile network generation. Additionally, in a mobile web attack scenario, the user’s data plan pays for the cost of the attack, so there is no financial disincentive for the attacker.

e) Credential risk: User credentials are constantly exposed with mobile browsers, as the user must sign in for every mobile banking session. This is the same exposure that exists with the online banking channel.

f) Customer-initiated only: The use of a mobile browser makes it impossible for the bank to initiate communications with the customer. This is due to the fact that the mobile phone’s interface is single-threaded, and therefore the application can not run constantly in the background.

Client Applications

Some vendors are now providing solutions that employ downloadable client software. This approach brings several benefits as well, including a) the ability for customization, b) a high level of branding and c) lesser charges for data plan access compared with mobile browsers.

However, this approach also comes with its own set of problems:

a) Operational Challenge: Forcing users to download, install, learn and gain familiarity with a custom application complicates the rollout and ongoing support. To address this problem, various carriers are now beginning to pre-install some applications, but the arrangement is limited to very few phones (and hence very few customers) and raises support issues (i.e. who does the customer call for support and product updates: the bank, the carrier, the software vendor or the phone manufacturer?). It takes only a few calls in to customer service to negate the return on investment of this offering.

b) Limited Availability: With over 12,000 different handset configurations already in use worldwide, creating, deploying and supporting new software on mobile phones is an arduous task. There are currently 5 different mobile operating systems (Microsoft Mobil, RIM, Palm, Symbian, Linux), 3 different major application development environments (BREW, J2ME, Symbian) over 130 different hardware platforms and numerous carrier networks. The fundamental difficulties of developing applications to accommodate all of these mobile phone variations make widespread availability to all customers extremely difficult.

c) Vulnerability to attacks: As an application running on the mobile phone without a personal firewall, anti-virus software or other protections commonly found on PCs, custom software is particularly vulnerable to malware.

d) Cost factors: Because there are no widely-accepted standards for running client applications on mobile phones and thousands of different handset configurations to account for, developing custom client applications can be prohibitively expensive.

e) Credential risk: Credentials are exposed whenever the user signs in for a mobile banking session. Additionally, many users may opt to configure applications with convenient features such as auto-login, but these leave the user's account vulnerable should the phone be stolen or lost.

f) Customer-initiated only: As is the case with mobile browsers, it is impossible for the bank to initiate communications with the customer as the mobile phone's interface is single-threaded, and therefore the application can not run constantly in the background.

Existing Phone Software (e.g. SMS)

A third approach to mobile banking is to use the phone's existing text messaging and software capabilities. Virtually all of the phones in the market today have text messaging (SMS) built-in and users are both fully "trained" and totally comfortable with their use. Such universal and intuitive operation—with no new mobile phone software or expensive data service required—is the hallmark of the ClairMail System.

In addition to leveraging any mobile phone's existing messaging capabilities, the innovative ClairMail System platform leverages other existing software and standard capabilities on mobile phones – including mobile browsers and Flash Lite. In this manner, the ClairMail System takes advantage of the strengths found with mobile browsers and client applications, while simultaneously addressing the various problems encountered with those approaches:

a) Universal availability: Works with any messaging-enabled mobile phone, regardless of manufacturer, operating system, platform or carrier.

b) No credentials at risk: Confidential information is never exposed during transport nor ever stored on mobile phones.

c) Multi-factor authentication: Out-of-band, transaction-level authorization provides additional strong security measures.

d) Leverages existing mobile phone software: Avoids the operational challenges (cost, support) and form factor issues found with other solutions.

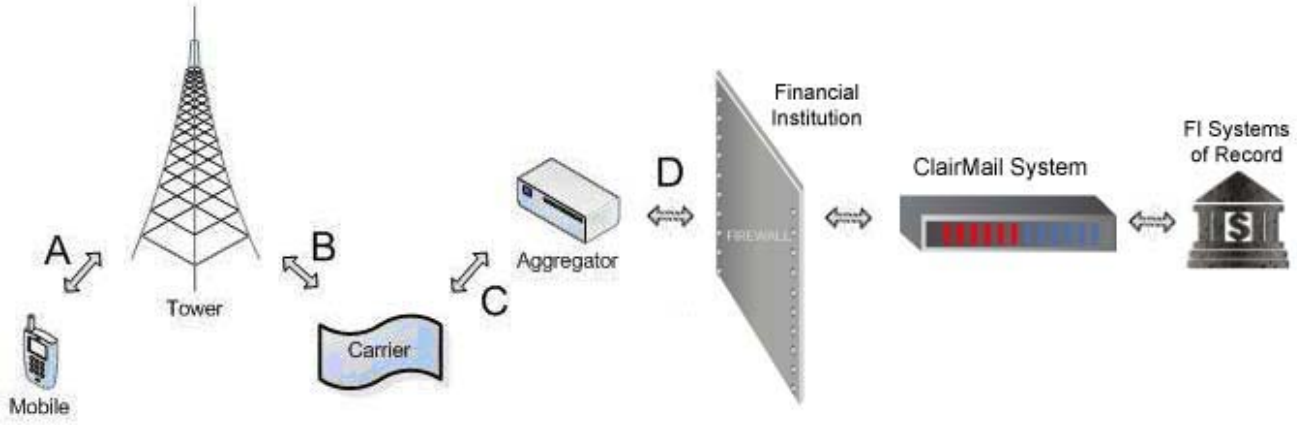
e) 2-way customer interaction: Communication can be initiated by either the financial institution or the customer.

> *"ClairMail improves wireless banking. Use of text messaging improves the likelihood of adoption. By eliminating the need for a Web-enabled cell phone and WAP connection, ClairMail's solution has eliminated some of the key problems with first-generation wireless solutions."*
>
> Brad Strothkamp
> Senior Analyst
> Forrester Research

f) Costly for attackers: Unlike other solutions where the user's data plan essentially pays for the attacker's costs, using SMS places financial barriers before would-be attackers—including short code acquisition, maintenance and per-message costs.

g) Not vulnerable to attacks: To be discussed in detail below, the ClairMail System addresses and answers all of the security issues surrounding mobile banking and payments.

Mobile Security Overview



The protection measures implemented by carriers and aggregators vary, and this white paper focuses specifically on the security provisions found in the ClairMail System and its seamless integration with the FI's systems of record. Nevertheless, it is useful to provide a brief overview of the security systems in place end to end, from the mobile phone to the ClairMail System.

A) Mobile phone to cell tower: Communications are encrypted from the mobile device to the cell tower. For instance, CDMA encryption is used to encode traffic on downlinks and uplinks, and time slots can be randomly assigned to the user. Additionally, the Global System for Mobile Communications (GSM) standard for mobile phones uses several cryptographic algorithms for security.

B) Cell tower to carrier: Dedicated copper connections from the tower to the carrier's private network, with encryption technologies applied at various places along the path. Carrier variations are possible.

C) Carrier to aggregator: Aggregator networks are similar in nature to the carrier networks. There is typically either a dedicated connection or a VPN connection from the carrier to the aggregator.

D) Aggregator to ClairMail System: The ClairMail System is installed on-premise, behind the financial institution's firewall or in a highly secure managed service environment. The ClairMail System establishes an outbound connection, encrypted and authenticated (typically SMPP over SSL and/or a dedicated connection), to the aggregator.

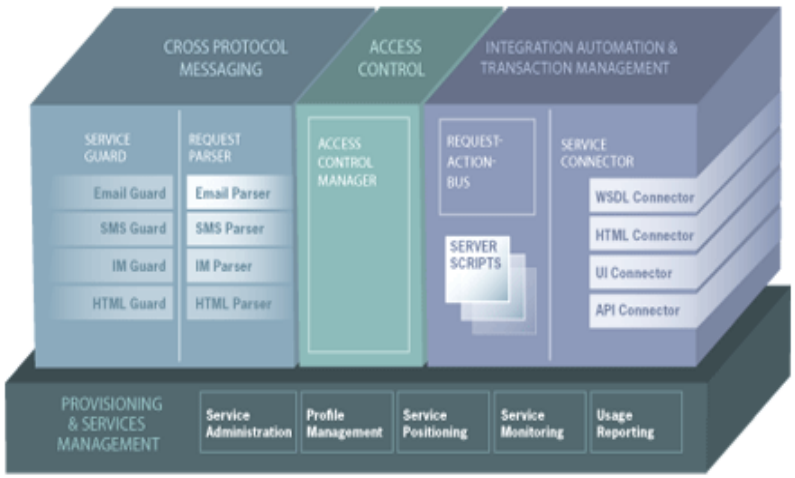
ClairMail System Security

The ClairMail System employs many layers of security designed to protect both the FIs' customers and IT infrastructure.

When the ClairMail System is deployed on-premise behind the FI's firewall, it seamlessly integrates with the FI's systems and is able to take full advantage of all existing layers of security in the enterprise network, including intrusion prevention systems, event monitoring, anti-virus and border security mechanisms.

Alternatively, the ClairMail System may be hosted as part of a highly secure managed service.

ClairMail System Architecture



Robust security provisions are integrated throughout the ClairMail System architecture.

Identity

A customer using the ClairMail System must enroll his mobile device with the FI offering the service. Enrollment typically takes place in one of four places: a branch office, the IVR system, the online banking application or mobile registration. All of these capture points provide the mechanisms to authenticate the customer *before* enrolling the mobile phone number and thus establish a "trusted path" of communication between the FI and its customer.

Once a customer has been authenticated, the following two pieces of information are required from the customer to complete the enrollment process:

1. User's mobile phone number.
2. The one-time, time-expiring PIN that the ClairMail System will send to the mobile phone number as part of the enrollment process.

For user-initiated requests, there is a base level of authentication that takes place by mapping the mobile number that the message is from to an enrolled user of the ClairMail System. This is adequate authentication for many transactions, given that cloning has been virtually eliminated for all digital mobile phones and the fact that only private data is being sent.

The ClairMail System also supports escalated authentication or authorization. Higher risk transactions – such as transfers, or transfers over a certain amount or between specific accounts –take advantage of this escalation. Escalating authentication is implemented as a two-factor authentication process. "Something I have" (the first factor) is the enrolled mobile device. "Something I know," (the second factor) for example, would be a PIN number. The escalated authentication can be used to create an authentication session (e.g., authenticate once, use same credentials for all transaction in the next 5 minutes) or on a per-transaction basis.

Escalated authentication crosses communications protocols to perform out-of-band verification of a transaction. Depending on the use case, this may use an outbound IVR call requesting a PIN following a mobile SMS transfer request, a WAP push message sent to accept that password in an SSL secured connection, or an actionable alert used for online and offline transaction verification.

Outbound messages (alerts, bill presentment, etc) are sent to the registered and validated phone number for the customer which was obtained at enrollment – the trusted path. Depending on the message, different levels of multifactor authentication, including escalating authorization, are used.

Multifactor Authentication

The popularity of online access to financial accounts has motivated regulators to provide security guidelines. Of particular importance are the guidelines for multifactor authentication specified by the U.S. Federal Financial Institutions Examination Council (FFIEC). These guidelines, which require two or more factors of identity when authenticating users, are outlined in an FFIEC document titled *Authentication in an Internet Banking Environment*. While the current version does not yet address mobile access explicitly, the importance of multifactor authentication remains the same.

The ClairMail System's transaction-level, multifactor authentication system has been designed to meet and exceed FFIEC requirements. With the ClairMail System, the first, physical factor (what the customer "has") is provided by the mobile phone itself—eliminating the need for cumbersome tokens, fobs, smartcards, biometric scanners or other such devices. The second, secret factor (what the customer "knows") can be a personal identification number (PIN) or a one-time password (OTP). This transaction-level authorization can occur out-of-band, for an additional level of security.

Below are two examples of multifactor authentication utilizing the ClairMail System. There are numerous scenarios to which multifactor authentication could be applied; these examples are not meant to be exhaustive, but merely illustrative:

Example 1: Escalating authorization of a transaction initiated from the mobile device.

1. User initiates a transfer from the mobile device via text message.
2. User receives a text message back from the system that he/she will soon receive an automated call back from the bank to authorize the transaction.
3. User receives a phone call from the bank IVR system. The user is asked to provide their PIN number to authorize the transaction.
4. User receives a confirmation message that the transfer has been authorized and will be processed.

Example 2: Escalating authorization of a transaction initiated from an online banking session.

1. User initiates a transfer within an online session by pressing the “submit” button.
2. A one-time, time-expiring password (OTP) is sent to the enrolled mobile number.
3. A screen in the online session prompts the user for the OTP that was just sent to the mobile device.
4. The user enters the OTP and the online transaction is allowed to proceed.

In each case, the customer actively participates in verifying the legitimacy of the transactions, a key ingredient in mitigating fraud and identity theft, as well as for non-repudiation.

Trusted Path Validation

Trusted Path Validation is used to ensure that every account is associated with a valid source address (e.g. a phone number or text messaging address). Customers can validate their address(es) in a number of ways, including a secure website, a transaction with multifactor authentication or in person. Any new address (e.g. a change to or the addition of another address or phone number) requires its own Trusted Path Validation process. Naturally, the actual source or “From” address of the message used is always matched with the address being validated.

Service Guard

Service Guard provides a layer of security checks that can be performed on a protocol specific basis. Recognizing that mobile communications capabilities and protocols will continue to evolve over time, ClairMail designed the Service Guard module in a manner to ensure that it is extensible to new messaging formats and the security mechanisms that will accompany them.

Encryption

Encryption is used throughout the ClairMail System, for both data in flight and data at rest. SSL and HTTPS encryption is used for data in flight (e.g. during SMPP connection to the aggregator and XML APIs).

Two types of data at rest exist in the ClairMail System:

1. Users’ mobile profile data.
2. Message data.

Users’ mobile profile data is always stored encrypted, using the Blowfish Encryption Algorithm. For message data, FIs have the option not to record message data into their system log files, removing any possibility of the log files being stolen. If FIs opt to record the message data, the log files are stored encrypted, again with the Blowfish Encryption Algorithm.

It should also be noted that, despite encryption being employed throughout the ClairMail System, there is still the real possibility of a mobile phone being lost or stolen. The ClairMail System addresses this vulnerability by never transmitting or storing any confidential information on the user’s phone, and ensuring that all private information sent shields personal details (e.g. full account numbers are never sent). Finding a lost or stolen phone would be equivalent to finding an ATM receipt.

Hardened Linux

The ClairMail System has the option of being delivered as a “hardened” Linux appliance, to provide yet another layer of security. The hardened Linux kernel in the ClairMail System server software minimizes vulnerabilities through careful security configuration and by utilizing only those modules that are required by the ClairMail System. Simply put, the fewer the number of software processes running, the fewer opportunities would-be hackers have to exploit the system.

Multi-Modal Integration

As an added security feature, the ClairMail System can be used to initiate a mobile Web banking session. To do so, the customer sends a text message through their mobile phone that includes a code word (e.g. Login). In response, the customer would receive a text message which automatically launches a mobile browser session that requests his login PIN. The mobile banking session begins after submission of login credentials. Because the customer initiates the mobile banking session by first sending and receiving text messages via the trusted path, he is assured of reaching the correct – and not a fraudulent – website.

Mobile Transaction Risk Scenarios

There are risks involved in many financial transactions. For example, handing a credit card to a total stranger in a restaurant exposes the account number, expiration date and the supposedly "secret code" on the back. However, when done properly, mobile transactions can be highly secure.

Presented here are some of the most common mobile transaction risk scenarios, and how the ClairMail System addresses each. By adhering to the "ClairMail Top 10 Tenets of Security Best Practices" (see sidebar), the ClairMail System provides industry-leading protection against these and other potential vulnerabilities.

Intentional Attacks

Attacks today can clearly have a profit motive. The techniques (SMiShing, phishing, vishing, spoofing or redirecting messages, and man-in-the-middle session hijacks, among others) are not the same, but the intent is financial gain from identity theft or fraud. To minimize the risk presented by these attacks, the ClairMail System employs rigorous access control with transaction-based and session-based escalating authentication and address validation (i.e. trusted path messaging). The ClairMail System server itself is protected by both its Service Guard module, its deployment behind the financial institution's firewall and its hardened Linux kernel. Finally, there are economic hurdles placed before would-be attackers, such as expenses for acquiring short codes (ranging in the thousands of dollars) and per-message costs.

Questionable Account Activity

A common symptom of a fraud or identity theft attack is suspicious or questionable account activity. The ClairMail System seamlessly integrates with the financial institution's fraud profiler systems, so dubious account activities are immediately identified and flagged. In these instances, the ClairMail System would deliver an out-of-band "actionable alert" to the customer's mobile phone requiring a response to authorize the transaction. Attackers attempting to spoof a customer phone for malicious purposes would be foiled, given that the actionable alert and all other communications would be sent to the real customer's phone via the trusted path. This process is not burdensome for the customer and, in fact, helps to mitigate fraud by actively involving customers in the protection of their accounts.

ClairMail Top 10 Tenets of Security Best Practices

The ClairMail System was designed to adhere fully to these fundamental tenets of solid security, together constituting a Best Practices of mobile security:

1) Confidential information is never transmitted over an insecure link.

2) All private information transmitted shields personal details (e.g. account numbers).

3) Nothing confidential is ever stored on the customer's mobile phone, especially access credentials.

4) Personally-identifiable information and access credentials are never exposed or put at risk (being stored instead in an encrypted database on the ClairMail server behind the firewall).

5) IT security personnel have full control over customer profiles and per-transaction security provisions.

6) Authentication, including multifactor authentication, can be required for any (or all) transaction(s).

7) All one-time-passwords (OTPs) are transmitted separately, out-of-band from the original request and securely on the carrier's network.

8) Existing infrastructure, such as IVR and other online systems, can be integrated to provide additional layers or levels of security. HTTPS encryption is used when utilizing the mobile browser.

9) All transactions can be logged beginning-to-end to provide a complete audit trail.

10) Invalidate any address or phone number no longer assigned to a customer and update/validate new ones.

Lost or Stolen Mobile Phones

With some mobile access solutions, having a phone stolen is tantamount to identity theft, with the thief now in possession of at least one, and potentially two, authentication factors. Client solutions are particularly susceptible to this problem (even poison pills can be negated if the thief simply disables access to the wireless network). Recognizing the frequency of lost or stolen phones, and the potential for disastrous results, the ClairMail System never stores anything confidential on the user's phone—not in the contact list, not in the mailbox, not anywhere on the mobile device. Instead, all such credentials are maintained in an encrypted database on the ClairMail System server, which resides behind the firewall and is protected by additional layers of security. In effect, this makes stealing a cell phone akin to finding an ATM or credit card receipt: no user credentials are exposed and no potentially exploitable information is provided.

Cloning

Since the implementation of the CAVE algorithm for digital phones, beginning in 1996, cloning fraud has been virtually non-existent on digital mobile phones. As the percentage of analog mobile phones has declined to low single digits, the incidence of cloning fraud on analog phones has also declined as a result of the infrequency of analog phones accessing the wireless network and being susceptible to being scanned for MIN/ESN information. Cloning fraud has not been an issue for at least the last seven years and there is no reason to believe that this won't continue to be the case.

Denial of Service (DOS)

There are multiple barriers which make a DOS attack unlikely to succeed against the ClairMail System. The first is financial disincentive, as there is a cost associated with sending each individual SMS message; launching an attack that would have a chance of saturating a system would be prohibitively expensive. Secondly, text messages bound for the ClairMail System stop at the aggregator first, at which point the ClairMail System establishes a secure polling connection to the aggregator to retrieve the messages, so there are no ports open to attack. Mobile Web and email are the only open ports, and the ClairMail System employs modern DOS prevention measures to thwart any attacks launched against them. Finally, the ClairMail System can be configured to only retrieve a pre-determined number of incoming messages per session established with the aggregator.

ClairMail System Security Challenge

The table below provides a summary of how the ClairMail System addresses the potential threats involved in mobile banking when leveraging messaging, and how it enhances security when leveraging mobile browsers and client applications.

Potential Threats	Messaging-based Security	Enhanced Security for Mobile Browsers & Client Applications
SMiShing, Phishing or Vishing	Transaction-level out-of-band, multifactor authentication. Expensive for attacker due to short code acquisition, maintenance and per-message costs.	SMS messages with correct links for initiating Mobile Web sessions or to download applications/upgrades can be sent via trusted path. This minimizes susceptibility of users being lured to fraudulent websites (which may trick them into providing confidential information, installing a malicious application or erroneously updating/ configuring their application).
Spoofing/Redirecting Messages, Man-in-the-Middle (MITM) Session Hijacks	Trusted Path Validation with out-of-band multifactor authentication make MITM and spoofing virtually impossible.	Transaction-level out-of-band, multifactor authentication make MITM and spoofing virtually impossible.
Malicious Code (Malware)	Plain text messages (SMS) can not carry viruses/malware. No downloading eliminates possibility of picking up virus/malware.	SMS messages with correct links sent via trusted path minimize susceptibility of users being lured to fraudulent websites (where they can be tricked into downloading viruses/malware).
Suspect or Questionable Account Activity	Outbound, 2-way "actionable alerts" actively involve users in fraud mitigation and transaction approval.	Adds capability for easily issuing 2-way "actionable alerts", which is otherwise impossible with mobile browsers and client applications.
Lost or Stolen Phone	No confidential information stored on mobile phone. Only private information sent/stored, with personal data shielded.	SMS messages sent with OTP and time-expiring, encrypted links for mobile browser or application sessions are no longer functional after their one-time use.

Non-repudiation

While FIs benefit by offering their customers online and mobile access to accounts, some of the transactions are ultimately challenged. The same is true, of course, for some credit card charges. To defend against such challenges, the ClairMail System validates user transactions, provides detailed audit logs, and preserves message delivery records. These provisions, along with multifactor authentication, meet FI non-repudiation requirements.

Conclusion

ClairMail recognizes the need to balance universal access, ease-of-use and strong security. As the only platform capable of leveraging the existing software and standard capabilities built into virtually all mobile phones, the ClairMail System utilizes a familiar, intuitive and ubiquitous means for mobile access. With the simplicity of ClairMail's secure mobile single-sign-on process, customers can access multiple accounts and perform a multitude of transactions. Once authenticated, customers can check account balances, transfer funds, pay bills, view transaction history or make any other authorized transactions—simply and securely.

To ensure that this powerful capability is fully secure and meets FFIEC guidelines, ClairMail has gone to great lengths to implement multiple layers of security, to adhere to demanding best practices tenets of security and to provide the means to manage the risk posed by all-too-common potential threats. By establishing a trusted path between customer mobile phones and back-end systems of record, the ClairMail System gives FIs a rapidly deployable, cost-effective way to offer a comprehensive and secure suite of 2-way mobile customer interaction services to all of their customers.

No other mobile access solution available today is at once so simple to use and so secure to operate.

To request a demonstration, or to learn more about how your organization can empower your customers with simple, secure 2-way mobile access to their accounts, visit ClairMail at www.clairmail.com, send an email to info@clairmail.com or call (415) 884-7270.