



White Paper

FrontBridge Secure Email: Technology Overview

Introduction

The Internet has enabled enterprises to move critical business processes onto the public network, improving communication and collaboration, strengthening partner relationships, and reducing operating costs. Through a proliferation of services and applications, the ability of enterprises to share data and collaborate with important constituencies beyond corporate boundaries – with customers, suppliers, and partners – has exploded.

As a result, the volume of traffic generated by the ever-increasing number of applications, including email, Instant Messaging (IM), web services, Voice over IP (VoIP), and other network transactions, has grown exponentially, and shows no signs of abating. Together with these applications has come an associated proliferation of the number of user identities within enterprises – email addresses, IM handles, VoIP telephone numbers, all of which need to be managed. At the same time, companies are under increasing scrutiny to adhere to government regulations and other compliance requirements to protect the privacy of customers, employees, and their personal data.

The traditional infrastructure used to protect data and communication based on certificates, commonly called Public Key Infrastructure (PKI), was not designed to deal with inter-enterprise communication, let alone the massive volume of data from an ever-growing variety of connected devices in the Internet-enabled era. Implementations in Fortune 1000 organizations have shown that PKI systems have a high barrier to use, leading users to shun them. Additionally, they are difficult for administrators to manage. PKI solutions have a high cost, often making them difficult for a CIO to justify for purchase and deployment.

The discontinuity created by the hyper-growth of the Internet as a business communication medium, the lagging usability of PKI, and the proliferation of identities across the growing range of business applications results in the clear need for a security platform that addresses these trends without introducing additional complexity. What is needed is a platform that enables enterprises to reap the full

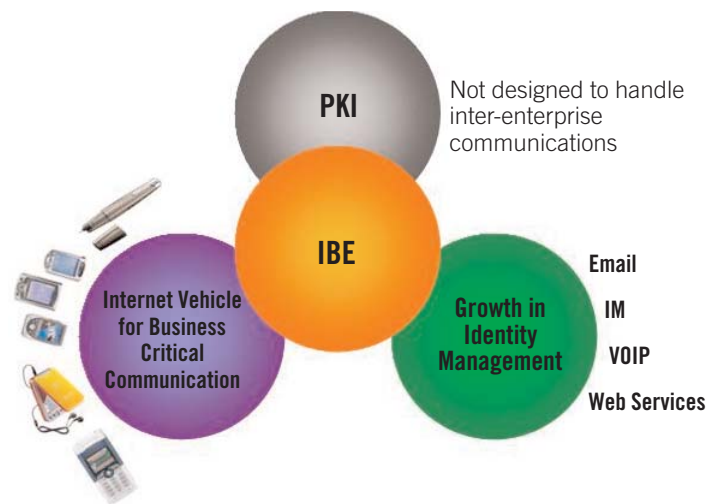


Figure 1 – Understanding the discontinuity

benefits of moving business processes to the Internet while simultaneously meeting compliance regulations, using a single, universal, easy-to-use encryption technique to secure all business communication in a simple and scalable manner.

FrontBridge Technologies has partnered with Voltage Security, Inc. to bring a new message encryption platform to the enterprise message management market. Based on a breakthrough encryption technology called Identity-Based Encryption (IBE), FrontBridge enables enterprises to conduct secure, scalable communication and fully experience the benefits and ROI of moving business processes to the Internet.

This paper will:

- Describe the existing encryption solutions and detail their inherent shortcomings;
- Define the critical requirements for a solution that enables ubiquitous secure business communication;
- Describe a groundbreaking new technology, called Identity-Based Encryption (IBE), that addresses these critical requirements and enables universal transparent secure messaging; and
- Illustrate how IBE technology is integrated into FrontBridge Secure Email and describe how this service enables businesses to easily send and receive ad hoc encrypted communication.

Shortcomings of Existing Network Security Solutions

Many attempts have been made to solve the problem of establishing trusted business communication – from the earliest use of symmetric cryptography in the 1970s through the current PKI (public key infrastructure) standard.

Symmetric Cryptography

Beginning in the 1970s, military and academic networks – precursors of the modern Internet – were the early adopters of modern cryptography, using security systems built on top of the first publicly available cryptosystems based on "symmetric cryptography." These symmetric cryptosystems, the best known of which is the Data Encryption Standard (DES), were widely used through the 1970s and are still used today as a component of modern cryptographic protocols.

In a symmetric cryptosystem, both the sender and the receiver use the same key. For example, if Alice wants to send a message to Bob, they meet in person and agree on a password. They can then use that password as a key to encrypt a message.

Implementations of symmetric cryptography, such as Kerberos, issue each user a password known both to the user as well as to a central server. So, if Alice wants to send a message to Bob, the following steps occur (see Figure 2 below):

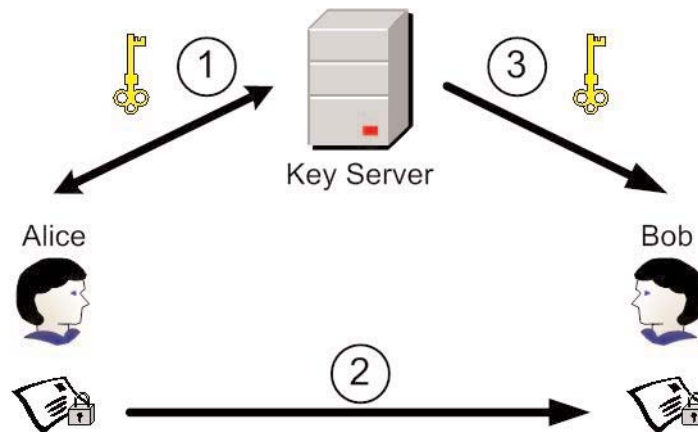


Figure 2 – Symmetric cryptography

1. Alice sends a request – encrypted with her password – to the server, containing Bob's name.
2. The server then generates a random key, and encrypts it with Bob's password. It also encrypts the key with Alice's password, and sends both password-protected keys to Alice.
3. Alice then encrypts the document with the random key, and sends the message and the other encrypted key to Bob. Bob can then decrypt the document.

Symmetric cryptosystems exhibited three critical shortcomings as the Internet and the need to secure communication and transactions grew.

Scalability issues quickly surfaced – Symmetric cryptosystems are inflexible and difficult to manage outside of small groups of users because a central server must be involved in the transmission of every communication in the system. When any pair of users wishes to send messages, they must communicate with the central server. As the number of messages and users in the system increases, the server gets more and more busy, creating serious scalability issues.

Strict online requirement eliminates offline capability – The need to communicate with the central server to establish a connection also requires that both the sender and the central server are online and able to communicate at all times. If the server is down or the user is offline, secure communication is impossible.

Interconnection is difficult – Interconnecting partner systems using symmetric cryptography can be difficult, if not impossible. Key translation servers or active trust brokering servers are required to interconnect one enterprise's trusted servers with another. This can be prohibitively expensive and may also require establishing a trusted third-party intermediary.

Asymmetric Cryptography

While symmetric cryptography was adequate for small, contained networks with a small number of users, it could not handle the volume of traffic brought on by the Internet boom in the 1990s. Handling this volume motivated the use of a newer form of cryptography that did not require online servers to broker keys for all users, called asymmetric or public-key systems. Commonly referred to as PKI, asymmetric systems were introduced to the market in the 1980s. In the PKI model, different keys – a public key and a private key – are used to encrypt and decrypt messages.

The encryption policy – specifying which users can connect to specified network resources, or which user can read email from a specified sender – is created by defining policy elements such as user names, network addresses, and trust levels. These policy elements are then coupled with the user's identity to their public keys – the product of two randomly generated prime numbers – via a "certificate."

Certificates are electronic documents that contain the name of the owner of a key, some information about the validity of the certificate (for example, a time period over which the certificate is valid), and the owner's public key. The owner's certificate is then electronically signed by a trusted authority called a Certificate Authority (CA).

In such a system, if Alice wants to send an encrypted message to Bob, the following steps are necessary (see Figure 3 below):

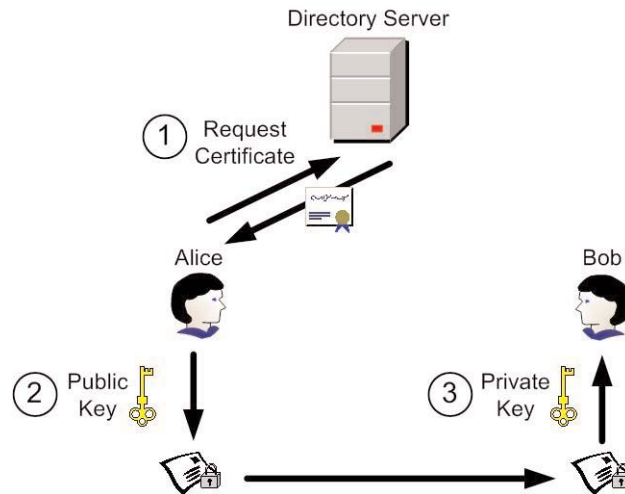


Figure 3 – Asymmetric cryptography or PKI

1. Alice contacts Bob – or a directory server – to obtain Bob's certificate, containing Bob's public key.
2. After locating Bob's certificate, Alice then downloads his certificate, validates the certificate against published revocation lists, validates the certificate's signing chain, extracts the public key, and uses Bob's public key to encrypt the message to Bob.
3. Bob receives the message then decrypts the message using his private key.

In theory, PKI should handle authentication of users and services flexibly and without limit with respect to the complexity of the policy. In reality, however, PKI has collapsed under the administrative weight of certificates, revocation lists, and cross-certification problems.

Five critical shortcomings and flaws exist in PKI that have prevented the technology from enabling ubiquitous secure messaging:

Certificates are not easily located – Before communication can take place, the client needs to locate a certificate for the message recipient. The lack of a standard directory that publishes certificates can make finding these certificates difficult – or impossible – even if both communicating parties are online simultaneously.

Strict online requirement removes offline capability – Closely related to the certificate issue is the requirement that users be online to conduct secure business communication. In the case of email, or in situations where both the client and server are offline, the user can only access and use certificates that have been cached on the sender's local machine, limiting communication to a small number of people for whom the user has certificates.

Validating policy is time-consuming and difficult to administer – Once a certificate is located, a client must validate the certificate, ensure that the certificate issuer is trusted, and match the certificate policy with the client's own policy requirements. This can be enormously time-consuming and difficult to administer.

For example, validating a certificate requires determining whether the certifying authority has revoked the certificate. Certificate authorities do this by either publishing a Certificate Revocation List (CRL), or by having the client contact an online revocation server. If the client is not online, this approach is rendered useless, because online revocation servers require that the client be online.

As the increased security requirements of Web services translate to an increasing number of properties that can, and will be, put into certificates, this problem becomes even more difficult. With more properties added to certificates, policies become more complex and already-massive Certificate Revocation Lists grow, leading to increased certificate volume and management overhead.

Certificates leak data – Since they must be accessible to clients, certificates publish a vast amount of information about the certified entities to the world, making them inherently insecure. Each application or person accesses and reads the certificate database of a large enterprise can construct a record of employee names, server names, and security status of those entities. Making this data accessible enables stronger security through better, more detailed policy decisions, but it also paradoxically imperils system security by publishing a detailed map of the enterprise's users, data, and services.

Users must pre-enroll – Before a user can send, conduct, or receive a secure message or transaction, pre-enrollment is required to make the user known to the PKI system. This means that a user cannot send a secure email or conduct a secure transaction with a Web server that is not already known to the CA, limiting the community with which a user can conduct secure communication. This pre-enrollment requirement is a primary factor limiting the ubiquity of PKI.

Overcoming the Flaws of Existing Technologies

The fundamental problem of both symmetric and asymmetric cryptography is that they do not address the authentication of users and services based only on user identity, and they do not provide the flexibility needed for conducting large volumes of secure business communication. Applications should be able to identify the services to which they are connected and apply policies about those specific services without user intervention or

complex configuration requirements. For example, an email user should be able to dictate that only authorized recipients can view a message or an attached document. Services, too, must be able to reliably identify authorized users and the operations that those users are authorized to perform. For example, servers must be able to require that only supply chain collaboration partners can view inventory data.

It's clear that a different solution is required, one which overcomes the flaws of existing technologies and which addresses the critical requirements of secure communication beyond corporate boundaries. This solution must:

- Secure anytime, anywhere communication;
- Allow for self-provisioning to easily facilitate and conduct secure communication;
- Enable secure messaging that is transparent to users;
- Be easily managed by administrators; and
- Provide a low cost of ownership and operation.

A Better Approach to Secure Communication: Identity-Based Encryption

FrontBridge and Voltage Security deliver breakthrough technology that radically changes the way people can execute secure communication. This technology is based on a new form of public-key cryptography called Identity-Based Encryption (IBE) that utilizes commonly used identities as the user's public key.

By eliminating the need for individual per-user certificates, this IBE-based solution provides a highly scalable, universally inter-connectible method for secure communication that overcomes the flaws of existing approaches. Specifically, this solution provides:

Secure anytime, anywhere communication – Users can conduct secure business communication anytime, anywhere – even on the road. For example, a secure email can be encrypted or decrypted on a laptop even when not online. Users can conduct business securely – from anywhere in the world – because they can roam transparently, enabling complete flexibility in how, and when, users conduct their work.

Self-provisioning to conduct secure communication – User self-provisioning is enabled by eliminating per-user certificates and the related requirement to connect to third-party servers to verify these certificates before initiating secure connections. No pre-enrollment of users is needed to conduct ad hoc secure communication. Ad hoc secure communication enables users to securely exchange messages without having knowledge

of whether the other party is already enrolled or registered. This type of communication matches the way people normally interact over the telephone or with a fax machine. The ad hoc nature of secure communication makes this solution infinitely scalable for an enterprise.

Secure messaging that is transparent to users – By using a commonly used identifier – such as an email address – as the encryption key, this solution provides a simple yet highly secure method to encrypt business communication, thereby enhancing overall enterprise security. No additional steps or clicks are required on the user's part to ensure secure communication because the user is recognized by his email address or user login.

Easy management by administrators – This IBE-based solution allows administrators to centrally manage the security of their business communication. Policies used to secure business communication are enforced at the central key server and can be changed simply and automatically. The sender merely transmits his security requirements and the key server enforces them. Administrators are also given the flexibility of working with any leading authentication methods. Virtually any system or network object can be centrally managed and secured through one solution.

Low cost of ownership – FrontBridge provides a lightweight solution that integrates easily and quickly with existing enterprise application infrastructure. Because heavy infrastructure and third-party CAs are not required, implementation of secure messaging within the enterprise's infrastructure is simplified. In addition, instead of deploying a point solution for each type of business communication that must be secured, administrators can deploy a single platform to secure all types of business communication, ensuring a low total cost of ownership (TCO) for the enterprise.

The FrontBridge Secure Email Architecture

There are three components of the FrontBridge security architecture:

1. The IBE Algorithm

Adi Shamir, one of the inventors of the well-known RSA public key system, originally proposed the idea behind Identity-Based Encryption in 1984. However, with no workable method to solve the problem known at the time, IBE remained one of the major unsolved problems in cryptography. It was not until 2001, when Dr. Dan Boneh and Dr. Matt Franklin, professors of computer science at Stanford University and the University of California, Davis, respectively, invented a practical scheme based on elliptic curves and a mathematical construct called the Weil Pairing.

IBE is the enabling technology within the FrontBridge security architecture, similar to the RSA standard that is the enabling technology for PKI.

The mathematical construct that makes IBE work is a special type of function called a "bi-linear map." A bi-linear map is a pairing that has the property:

$$\text{Pair}(a \bullet X, b \bullet Y) = \text{Pair}(b \bullet X, a \bullet Y)$$

For IBE, the operator " \bullet " is the multiplication of integers with points on elliptical curves. While multiplication itself (e.g., calculating $a \bullet X$) is easy, the inverse operation (finding a from X and $a \bullet X$) is practically impossible. The bi-linear map that is used is a Weil Pairing or Tate Pairing.

The idea of the bi-linear map is then applied to the IBE algorithm (Figure 4). A key server generates a secret s and a parameter P using random number generation. Next, the public parameters, P and $s \bullet P$ (the product of s and P), are distributed to all users. Then, a private key is issued to each user by the key server. This private key is the product of the user's identity and the secret s . For user Bob, this is $s \bullet ID_{Bob}$.

2. The Key

Because IBE allows the user to choose his public key and receive his private key from a trusted, central source, FrontBridge users' public keys are their identities (e.g., email

Sender (Alice)	Receiver (Bob)
To encrypt a message to Bob, Alice picks a random r and calculate a key k :	After receiving the message, Bob can reconstruct the key k by calculating:
$k = \text{Pair}(r \bullet ID_{Bob}, s \bullet P)$	$k = \text{Pair}(s \bullet ID_{Bob}, r \bullet P)$
We now send to Bob $E_k[\text{Message}]$, the message encrypted with k . We also send him the product $r \bullet P$.	and decrypts the message with it. As Bob is the only person who knows his private key $s \bullet ID_{Bob}$, no one else can calculate k .

Figure 4 – Sending and receiving a secure message with IBE

addresses or network logins). This seemingly simple but technically difficult breakthrough makes certificates superfluous and ties security policy directly to the encryption or authentication method.

The following examples illustrate the difference between keys in a public-key system and those in the FrontBridge solution. Figure 5 shows a public key for the RSA algorithm. Because the key is a number several thousand bits long, it does not have a concept of identity. As a result, a certificate is needed to tie the public key to an identity.

The sender must have all this information and connect the information via a certificate to the recipient to send a secure message.

```
Public exponent:
0x10001

Modulus:
13506641086599522734960321627980596993892147560566702752448514385152651060
48595438339402871505719094517982072821644715313736804197039641917430464965
89274256239341020864383202110372958725762358509643110564073501509187510623
59462920556368552947521351595287941637732853390610975054433421981115005697
7236890927563
```

Figure 5 – An example of an RSA Public Key

In contrast, Figure 6 illustrates a public key using IBE:

```
Name = bob@b.com
```

Figure 6 – An IBE Public Key

The ability to choose simple, understandable keys underlies the power of the FrontBridge architecture to encode policy directly into encryption and authentication methods.

3. Key Management

Key management encompasses two primary functions: key generation and key updating. These responsibilities are handled completely by the FrontBridge servers – no server hardware is required on the customer's premises.

Key generation is the function of generating the public and private keys for use in secure communication. Key updating insures that keys are changed regularly, thereby protecting the system and the user if a key is lost or stolen.

Key Generation

The FrontBridge Key Server's primary function is to generate private keys in an IBE-based security system and to enable users, services, and applications to use IBE encryption.

Key Update

Key update is the component of key management that ensures the validity and authenticity of the key. To prevent against key compromise, FrontBridge uses a combination of an identity and the date, such as:

"name=Bob validity=09/1/04-10/01/04"

Since the public key is different for each time period, so is the corresponding private key. This automatically limits potential key compromise to the duration of the original key. Furthermore, instead of revoking a key for a fired employee or compromised machine, the FrontBridge Key Server simply stops issuing private keys to that identity.

In contrast, key compromise in PKI-based systems is handled by placing the corresponding certificate on a Certificate Revocation List (CRL). In practice, most clients do not check CRLs and therefore compromised keys remain undetected.

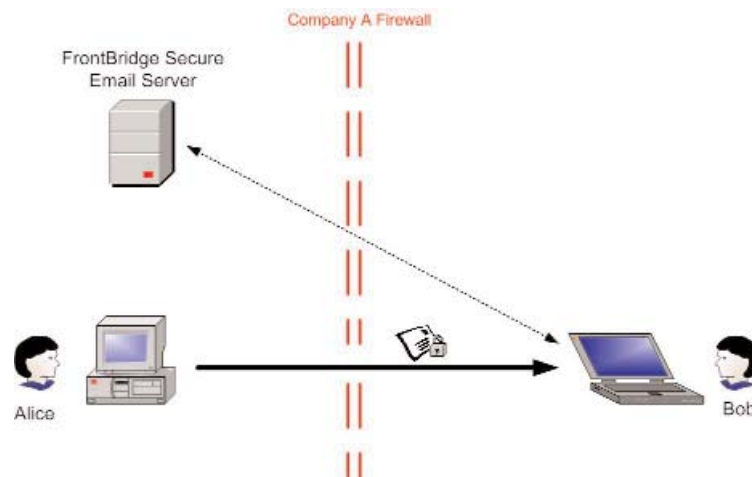


Figure 7 – Sending a secure email using FrontBridge Secure Email

How the FrontBridge Solution Works

Alice at Company A wants to send a sensitive email to her customer, Bob at Company B. For compliance reasons, the email must be secure. Alice uses FrontBridge Secure Email to send the message to Bob.

Alice Sends a Secure Message to Bob – With the FrontBridge Secure Email plug-in installed on Alice's machine, she composes the message and simply clicks the Send Secure button in her email client. This action automatically secures the message, along with any attachments, using Bob's email address bob@b.com.

FrontBridge Secure Email does not require pre-enrollment of users to receive secure email; even if Bob has never previously communicated with Alice or has never used FrontBridge Secure Email, he is still able to receive secure messages from Alice.

Bob Receives the Secure Message – The first time Bob receives a secure message on his laptop, Bob clicks on a link in the message header and downloads the FrontBridge Secure Email plug-in. He then proceeds to enroll and authenticate to the FrontBridge Secure Email server. The method used to authenticate Bob is completely flexible to the requirements of the enterprise.

Bob Decrypts and Views the Message – Upon completion of proper authentication, FrontBridge presents Bob with his private key to read the secure message. Alice and Bob can now communicate securely with FrontBridge Secure Email. In fact, Bob and Alice can communicate securely without making any network connections to the FrontBridge Secure Email Server.

Further, with his private key downloaded to his laptop, Bob can decrypt and view his received secure messages even when he is offline. Bob can even read his secure email at a business center using FrontBridge Secure Email's transparent roaming capabilities.

Summary

Sending a secure email today, using a traditional email application combined with PKI, is complicated and presents many roadblocks, which is why the vast majority of email is not encrypted. Often, the sender only knows the recipient's email address, and must determine the recipient's certificate either by consulting a directory or by contacting the recipient directly. While directories do exist, they are not widespread, so consulting them is generally futile. If the sender must contact the recipient, this can create delays. Moreover, the request for the certificate is unprotected.

Another solution offered in the market today is web-based secure email. In this example, the message is stored on a web server and the recipient is notified of the message with a secure URL link. While its ease of use may be somewhat attractive, most email users are unwilling to switch to non-standard email clients. The inability to easily integrate one's email into standard clients breaks workflow and creates usability issues for users. Because the email is now stored on a Web server, the user is required to be online to view the email. Corporate email users require the ability to manage their email locally on their machines. A solution that places strict online requirements is not viable for enterprise email users.

In contrast, FrontBridge Secure Email enables users to send secure email directly to any recipient – instantly. If this is the first encrypted message received by the recipient, he simply contacts the enterprise key server to acquire the private key. Otherwise, he merely decrypts the message without any additional steps or effort.

Because FrontBridge overcomes the roadblocks to secure messaging and enables transparent encryption, enterprises gain better, finer-grained control over external communication. With fewer impediments to use, email encryption becomes second nature and more ubiquitous amongst an enterprise's email users, thus allowing the enterprise to audit email traffic and comply with government regulations.

Conclusion

FrontBridge Secure Email, powered by Voltage Security, delivers a revolutionary method for securing communication that overcomes the hurdles of existing solutions. As a result, FrontBridge helps enterprises experience the full benefits and ROI of moving business processes to the Internet.

By using a commonly-used identity – such as the user's email address or network ID – as the user's public key, FrontBridge is the only service-based, email security provider that addresses the critical requirements of ubiquitous secure communication beyond corporate boundaries.

FrontBridge offers a secure email solution that provides:

- Secure anytime, anywhere communication;
- Self-provisioning to easily facilitate and conduct secure communication;
- Secure messaging that is transparent to users;
- Easy management by administrators; and
- Low cost of ownership and operation.

FrontBridge's transparent encryption breaks down the barriers to secure messaging by making it second nature – thereby enhancing enterprise security. FrontBridge Technologies brings confidence to an enterprise's most sensitive business communication.

About FrontBridge

FrontBridge Technologies Inc. is the market leader for enterprise message management and email security. The company's SMART network – a proven, reliable, on-demand, globally-distributed network of secure data centers – provides a frontline of defense against spam, viruses and malicious e-mail-borne attacks with unmatched security, performance and reliability. FrontBridge was the first company to guarantee 99.999-percent uptime in service level agreements (SLA) and the only company with a track record of 100-percent uptime.

Now in its fifth year of operation with headquarters in Marina del Rey, Calif., FrontBridge provides message management and security for more than 2,000 enterprises globally. Our technical anti-virus partners include Sophos, Symantec, and Trend Micro. FrontBridge Technologies, Inc.

4640 Admiralty Way, Sixth Floor
Marina del Rey, CA 90292
(877) 301-8232 • (310) 302-0500
www.frontbridge.com