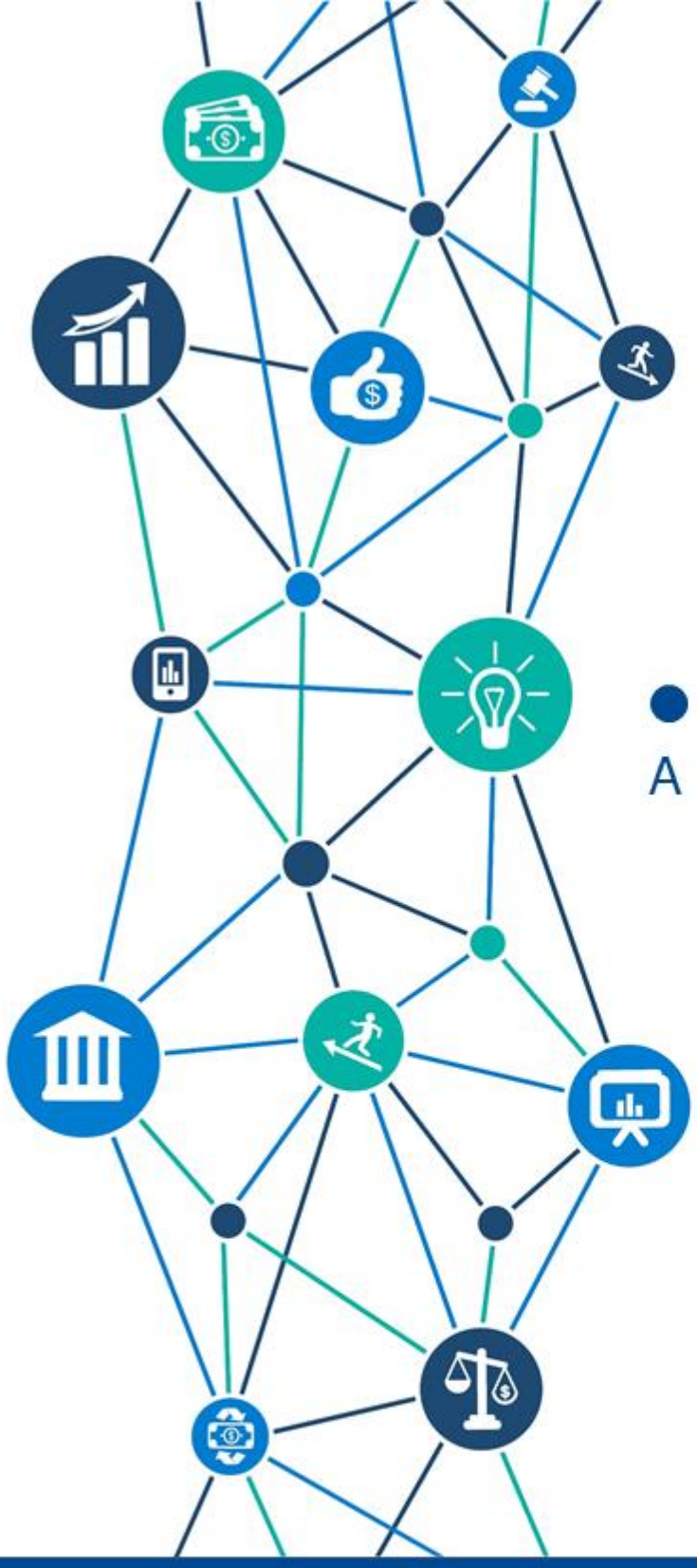

.BANK

A Business Case White Paper

ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

EnCirca
SOC 2 CERTIFIED

.BANK: A Business Case White Paper

I. Executive Summary

This white paper, written in partnership by the Independent Community Bankers of America (ICBA)[1] and EnCirca,[2] provides a general overview of the .BANK top level domain extension (".BANK," or ".BANK domain," or ".BANK domain name"), its purpose, and business case arguments. The .BANK domain is a more secure web domain for community banks and their customers when compared to existing domain alternatives. It helps protect both bank and customer data. The .BANK domain provides a competitive marketing advantage for community banks that adopt this new web brand. Several documented community bank success stories illustrate the ease of implementation and acceptance of the new domain by customers, employees, and other stakeholders.

The benefits of owning a .BANK domain name are ever growing. The more banks that adopt a .BANK domain name, the more recognition and trust the .BANK brand will gain. Even banks that purchase a .BANK domain for the purpose of redirecting traffic to their .COM website are able to build equity among the search engines while their web presence gains momentum and recognition. Those banks that fully migrate to a .BANK domain are able to reinforce their relationship with their customers through trust. Collectively, when banks migrate to the .BANK domain, they establish an easily recognizable brand with the same security and rapport in the financial industry as any of the largest banks.

II. Introduction

In today's age of cybersecurity threats and customer concerns about the safety of their data, employing a .BANK domain is an effective step that a community bank can take to assure its customers it is using the most enhanced methods available to secure their customers' online interaction (online, mobile banking and email) with the bank.

The .BANK domain is a protected, trusted, more secure, and easily identifiable brand on the Internet for the global banking community, and the customers they serve. The .BANK domain extension mandates enhanced security requirements, which are often overlooked in other domain extensions. For example, one feature of the .BANK domain is email authentication, which mitigates spoofing, phishing, and other malicious activities propagated through emails to unsuspecting users and recipients. This is an immense protection for all community banks, including those that may not have an online banking platform but communicate with customers via email. Another unique security feature is the multi-factor authentication requirement, which ensures that any updates to the bank's domain is made only by

[1] The Independent Community Bankers of America®, the nation's voice for more than 5,800 community banks of all sizes and charter types, is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education and high-quality products and services. With 52,000 locations nationwide, community banks employ 760,000 Americans, hold $4.7 trillion in assets, $3.7 trillion in deposits, and $3.2 trillion in loans to consumers, small businesses, and the agricultural community. For more information, visit ICBA's website.

[2] Formed in 2001 just north of Boston, EnCirca is a Registrar specialist focusing on brand protection and domain extensions that restrict eligibility to members of an industry or community. EnCirca continues this track record with the .BANK extension as the first ICANN Registrar serving on fTLD's Security Standards Working Group. Contact us to learn about our brand protection services and our .BANK-compliant Secure DNS and Email Authentication DMARC services. For more information, visit EnCirca's website.

authorized users. Additionally, enhanced encryption is required to ensure optimal data privacy and security. These are just a few of the security features from which banks immediately benefit upon implementing a .BANK domain.

The .BANK domain also provides new marketing and branding opportunities promoting the security of the bank to its customers. For these reasons, ICBA and EnCirca teamed up to educate and promote the value of .BANK domain names to community banks nationwide.

Until recently, only a few web domain extensions, or top level domains, were available for use, such as ".COM," ".ORG," ".EDU," ".GOV," and ".NET." In 2015, the Internet Corporation for Assigned Names and Numbers (ICANN) approved the use of .BANK, a new financial top level domain that is owned and operated by members of the banking industry, including the ICBA.

As of December 31, 2016, approximately 2,600 U.S. banks have registered a .BANK domain. Each bank owns, on average, approximately two domains. The renewal rate for the .BANK domain is approximately 84 percent and banks are beginning to renew their new domains for multiple years.

Each top level domain has a registry operator. The .BANK registry operator is fTLD Registry Services, LLC, whose sole mission is to operate the .BANK domain for verified members of the banking communities. fTLD has many resources available to community banks, including guides on leveraging a .BANK domain and an Implementation Planning Checklist. These resources are designed to assist community banks with the planning and implementation of a .BANK domain and include information on a communications plan for employees, customers, executives, technology teams and third-party service providers.

fTLD also maintains an approved Third-Party Provider Program for .BANK registrants. The program website lists third-party providers that can assist community banks in migrating their website to a .BANK domain and in complying with the security requirements necessary to support websites and email for a .BANK domain.

III. Business Case for Migrating to .BANK

The business case for the .BANK domain is simple: implementing a .BANK domain has both security and marketing advantages for community banks.

a. Comparing .BANK to .COM

As detailed below, fTLD Registry Services, LLC mandates many security features when obtaining and maintaining a .BANK domain that are non-existent in the .COM web domains. These mandatory requirements help convey to consumers that every .BANK website and email platform consistently follows the same security standards. The result provides consumers with peace of mind about the interactions they have with a .BANK website and email address. These security measures collectively help to eliminate any type of spoofing, phishing, or other malicious activities across the .BANK domain.

Some community banks are hesitant to adopt a .BANK domain until the largest banks do so. The largest banks have the financial resources to purchase, implement and support proprietary domain names which are typically their recognized brands. Additionally, these banks have various strategies for capitalizing on the domain expansion. At least one is employing their own proprietary

domain extension (i.e. ".CHASE") in addition to owning a .BANK domain. Alternatively, another bank has its own proprietary domain without owning a .BANK domain (i.e. ".BARCLAYS").

The .BANK domain allows a community bank to maximize the security of its domain without the substantial investments necessary when pursuing this initiative independently. By adopting a .BANK domain now, community banks establish a competitive marketing advantage over larger banks. First, they can secure a short, intuitive domain for their community bank. Short domain names in .COM were snapped up by speculators long ago, but there are still a large number of short generic names available in .BANK. Second, community banks employing a .BANK domain can positively demonstrate to their customers that they adhere to high security standards in protecting customer data. The ability to do that rests in the mandatory security requirements of maintaining a .BANK domain, which are typically unavailable or inconsistently followed for .COM websites.

This table provides an overview of the differences between a .COM domain and a .BANK domain:

Attribute	.COM	.BANK
Eligibility	No Restrictions	Restricted to verified banks only
Naming Allocation	No Restrictions, leading to spoofing and phishing	Must correspond to bank's existing rights
Encryption	Optional	Required
Domain Name System Security Extensions	Optional	Required
Email Authentication	Optional	Required
Multi-factor Authentication	Optional	Required
Short, Intuitive Name Availability	Very expensive on the aftermarket	Shorter, more relevant branding
Branding Association	No Restrictions, free-for-all, full of bad actors	Recognized as a vetted, trustworthy website

b. Security Features of .BANK

All .BANK registrants are required to implement robust, mandatory security requirements.[3] This requires some planning in order to obtain a smooth transition. According to fTLD's Success Stories (links below) and recent surveys, a full migration usually takes about four months. To expedite the process, some registrars have a turnkey solution that will stand up a fully compliant .BANK website within a month. For community banks, adherence to the security requirements will typically be accomplished by engaging a third-party provider to establish its .BANK domain. fTLD's Third-Party

[3] For additional information about the security requirements, please visit fTLD's website.

Provider Program will assist community banks in meeting these security requirements. The third-party providers that are able to assist community banks are listed on fTLD's website.

The .BANK domain accomplishes adherence to its industry-developed security requirements by providing authentication of a bank's identity through strict verification procedures and compliance monitoring by fTLD. The enhanced security requirements of the .BANK domain are continually reviewed through its industry-based Security Requirements Working Group. The working group is an on-going advisory group that meets regularly to review all security requirements. The group updates and improves upon the .BANK domain security standards in order to stay relevant in the continuously developing cybersecurity environment.

Requiring adherence to these robust security standards guarantees that all visitors to .BANK websites will be able to safely and securely transmit confidential information over a secure medium. These requirements include background checks prior to registration of a domain name, anti-DDoS measures through DNSSEC, Transport Layer Security/Secure Sockets Layer, DMARC authentication, secure web hosting, multi-factor authentication and ongoing verification standards.

i. Background Checks

These requirements start even before a domain name is registered. Symantec, a leading anti-virus and Secure Socket Layer (SSL) Certificate company, conducts rigorous background checks on all new .BANK domain applicants. These checks range from verifying that a registrant is authorized by the bank to apply for a .BANK domain to ensuring that the bank is a valid, *bona fide* bank.

Once an application is approved and a .BANK domain name is awarded, many more requirements commence.

ii. Domain Name System Security Extensions (DNSSEC)

Domain Name System Security Extensions, or DNSSEC, is the latest and more secure generation of Domain Name Servers, or DNS, which allows a website to connect to the Internet and translate an IP address into a plain text web address. The next generation of DNS/DNSSEC has increased security attached to it, protecting this vital connection. Unlike .COM and other domains, DNSSEC must be enabled at both the domain's DNS Name Servers and the .BANK Registry before a .BANK domain is allowed to go live on the Internet.

This highly redundant and scalable network helps fight against Distributed Denial of Service (DDoS) attacks. With the increasing voracity of these attacks against all industries and the growth of the "Internet of Things,"[4] this is an important protection. The goal of the hackers in a DDoS attack is to overrun a website's bandwidth, causing

[4] The "Internet of Things (IoT)", as defined by the U.S. Department of Homeland Security, are network-connected devices, systems and services. These devices may include anything from sensing, heating/cooling, lighting, motor actuation, transportation devices to information networks (including the Internet) via interoperable protocols, often built into embedded systems. While many benefits come from the innovation of connected devices, many risks are also prevalent. Hackers may seek to use the IoT in order to accomplish a DDoS attack against a website, for instance. For additional information, see the DHS website on IoT.

the site to crash, preventing all online activity. The attackers may then ask for a ransom while holding a site hostage. With DNSSEC, it becomes increasingly difficult for this type of attack to occur as the bandwidth load is distributed across numerous networks throughout the globe.

iii. Transport Layer Security (TLS) and Secure Socket Layer (SSL)

Another technical security requirement is the use of Transport Layer Security (TLS) and Secure Sockets Layer (SSL) Digital Certificates. These certificates secure the connection between a website and a website's visitors by creating an encrypted connection between a website and a visitor's computer. These digital certificates allow website visitors to share confidential information while they are on a site. All of the transmitted data during a site visit is encrypted, presenting large obstacles for malicious users to interfere and steal private information, such as login credentials and personal banking information.

iv. Domain Based Message Authentication and Conformance (DMARC)

A common attack in the financial industry comes from social engineering emails, or more specifically C-Suite email spoofing and phishing. No other top-level domain defends against these malicious attacks. With the .BANK domain, a form of email authentication known as Domain-based Message Authentication, Reporting & Conformance (DMARC) is required to help prevent these attacks.

DMARC is a requirement that involves the email addresses used by a bank to send outbound mail. DMARC is a way to determine whether a given message is legitimately from the sender, and what to do if it is not. This makes it easier to identify spam and phishing messages, and keep them out of customers' inboxes. DMARC provides domain-owners with control and the ability to block domain-based spoofing. Used correctly, DMARC also provides domain owners with intelligence, by giving domain owners aggregate and forensic data on emails. DMARC implementation is complicated and has traditionally been too costly for most small businesses. This service typically costs tens of thousands of dollars a year for a company to implement. However, with the advent of the .BANK domain, DMARC providers developed a significantly more affordable solution, specifically for .BANK registrants.

The .BANK requirement is that the domain must be in DMARC Alignment with either: a Sender Policy Framework, or SPF, a type of DNS record that identifies mail servers that send email on behalf of the domain; or, Domain Keys Identified Mail, or DKIM, a way by which spamming, spoofing and phishing is limited. The email service providers, such as Google, Yahoo, Comcast, and Microsoft read DMARC records to ensure that they do not deliver unauthorized email. This mandatory implementation further enhances the security of the .BANK domain by preventing malicious users from stealing information and gaining access to your infrastructure from both the bank's customers and employees.

v. Secure Web Hosting

Some vulnerabilities for those that operate a website containing sensitive information are found in the web hosting itself. The secure web hosting requirement for a .BANK domain mitigates these vulnerabilities through the disabling of certain, outdated ports and cipher suites. When the .BANK domain first launched, it was difficult for banks and service providers to find a vendor that could offer this security requirement because the hosting industry has remained fairly stagnant over the last decade in terms of security. In response to overwhelming demand, hosting companies upgraded their packages to offer secure web hosting. Thanks to the advent of the .BANK domain, secure web hosting is now found at most hosting companies. For a list of providers, please view the previously mentioned Third-Party Provider list.

vi. Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) for updates to domain data is a critical requirement as it prevents the most common form of activity by malicious actors, that may not only include outside hackers, but also insiders. Hackers attempt to re-direct a hacked account to a third-party website by changing the DNS name servers for the domain. The .BANK domain minimizes this occurrence by requiring multi-factor authentication. Multi-factor authentication ensures that any change of registration data is made only by authorized users of the registered entity. All of the significant changes below require MFA:

- Updating customer records;
- Changing and/or updating a domain's nameservers information; and,
- Updating "Whois" contact data.

Registrars implement MFA by linking domain name accounts to a bank employee's cellphone, computer, email, or an additional account. When a user attempts to change any of the information above, they are prompted to enter a MFA code, which can be found via the linked device or account. This helps prevent malicious actors from making vital changes to a bank's website.

vii. Ongoing Verification

The last and most crucial security requirement for the .BANK domain is the ongoing verification and vulnerability scanning performed by the fTLD Registry. fTLD actively monitors the top- level domain to ensure that all .BANK domain names comply with the eligibility and security requirements. This level of vulnerability scanning done for the .COM domain names of major corporate banks costs millions of dollars each year. However, with .BANK, there is no additional cost for scanning because it is built into the cost of each domain name.

Every .BANK registrant undergoes their eligibility background check every 20 months. This preserves the integrity of .BANK and maintains consumer trust by verifying that any website ending in .BANK is indeed a legitimate, secure banking entity. Ongoing scanning conducted in real time also enforces the security requirements. When a .BANK website is found non-compliant, fTLD Registry Services notifies the bank immediately. fTLD will help banks achieve a compliant website. However, for those banks that continually

prove an unwillingness to comply with the security requirements after several attempts, fTLD will remove the .BANK website. These actions guarantee that the .BANK domain continues to mitigate cyber-attacks and continues to be the most trusted domain name on the Internet for the banking industry and its consumers alike.

Unlike .BANK websites, consumers using a .COM site have no way of knowing the true security of how their information is transmitted since there are no common security standards.

Additionally, consumers cannot be certain that the website is the legal entity for which it appears (i.e. a spoofed website). However, these elements of doubt and uncertainty are eliminated by utilizing a .BANK domain due to its extensive verification checks, which eliminate all bad actors from the web community.

c. Marketing Considerations

.BANK is more than just a domain name; .BANK is a brand synonymously associated with the financial industry. The more exposure the .BANK brand obtains, the more valuable it becomes. When consumers see that banks are using the .BANK brand, they understand that it represents a higher level of security than a .COM domain name.

A .BANK domain name can also be used to shorten web addresses. Many corporations are already using their own top level domain for the purpose of shortening their web addresses. Shorter web addresses can redirect to a company's current website. This will simplify a bank's online presence, making their brand shorter, and more memorable for consumers.

Each community bank that implements a .BANK domain is instantly associated with an industry brand 2,600 banks strong. Automatically, the registrant must adhere to strict security standards which protects consumer information that is transmitted on the .BANK website.

In short, a .BANK domain name helps banks:

- Tell a security story their customers can understand;
- Ensure their customers that exposure to cyber threats for websites and email is mitigated; and,
- Enhance brand differentiation in a competitive marketplace.

IV. Additional Reasons to Adopt .BANK

.BANK offers numerous advantages to banks that have no plans in the immediate future to migrate to the BANK domain.

a. Defensive Purposes

A number of banks have registered a .BANK domain for purely defensive purposes. While this certainly protects a bank's brand from becoming diluted by another similarly named bank, those banks could achieve a better return on investment. For example, banks can realize Search Engine Optimization and marking benefits by redirecting their .BANK site to a .COM site.

b. Search Engine Optimization and Marketing

Search engines such as Google and Bing give greater weight in search results to websites that have greater longevity. The longer a website has existed on the Internet, the higher its search ranking. Inevitably, the .BANK brand and search result presence will continue to grow as more consumers become aware and demand it of their banks. The time is now to start building search engine equity while the .BANK brand gains momentum.

In addition to longevity adding to search engine equity, technology trends indicate that a .BANK domain will offer far more than the basic search engine optimization. Search engines are constantly looking for new methods to give more relevant results to end users. In the past, search engines have given preference to verified top level domains. Historically, search engines such as Google have ranked vetted domains, such as those similar to the .BANK domain, above non-vetted domains such as .COM.

c. The More the Better for Everyone

The end goal of owning a .BANK domain name is to migrate a current website to a new and improved .BANK website. Every bank that migrates to the .BANK domain contributes to enhancing the .BANK brand, creating a mutually beneficial environment that reinforces itself as the trustworthy, go-to domain name for all banking purposes.

After a bank makes the switch to their .BANK website, the final step is to migrate to .BANK email addresses. This further solidifies the website's integrity as not only are .BANK websites protected and secure, but .BANK emails are authenticated. As stated previously, one of the most common forms of hacking comes via email phishing and spoofing. With full DMARC alignment, all phishing and spoofing attempts are nonexistent from .BANK email addresses.

Nearly half of the banks in the United States own a .BANK domain name. Their .BANK domain name protects their brand name and gives them a competitive advantage over non-adopters. By adopting the .BANK brand, customers understand the security story and grow to recognize the .BANK domain as much as they may recognize the larger corporate banking brands. The .BANK domain is the perfect response from the community banking industry to solidify their relationship with their customers, aggressively dissuade hacking attempts, and collectively compete with the large corporate banking brands.

V. Case Examples

Several community banks have already deployed a .BANK domain and have shared their stories with fTLD. Below is a sampling of some ICBA member banks' success stories. There are several more available on fTLD's Success Story webpage. Following implementation of a .BANK domain, ICBA encourages community banks to share their success stories as well:

Badger Bank
Blue Ridge Bank
Bridge Community Bank
CNB Bank
Chelsea State Bank
Choice Bank
TrailWest

VI. Obtaining Additional Information

If you have additional questions, or would like more information the below representatives would be happy to assist:

ICBA	EnCirca
Jeremy Dalpiaz AVP, Cyber Security and Data Security Policy jeremy.dalpiaz@icba.org 800-422-8439	Andrew Barrett Product Manager andrew@encirca.com 781-942-9975

Additionally, these resource websites may be helpful:

fTLD Registry Services, LLC
Independent Community Bankers of America
EnCirca and the Independent Community Bankers of America.