# Protecting Critical Data in Your Financial Institution

## Capitalizing on Today's Data Security Challenges

WINMAGIC®
DATA SECURITY

# TABLE OF CONTENTS

WINMAGIC®
DATA SECURITY



# EXECUTIVE SUMMARY

Personally identifying information has become more fluid in the digital age, making it easier for thieves and hackers to access. Financial institutions in particular are high priority targets due to the monetary gain at stake, so these organizations must prioritize the protection of customer information through the use of data encryption to maintain strict security. Those that do not employ stringent data security measures, face severe consequences should they break the trust of their customers and business partners or violate a variety of regulations they must observe locally, regionally or worldwide.

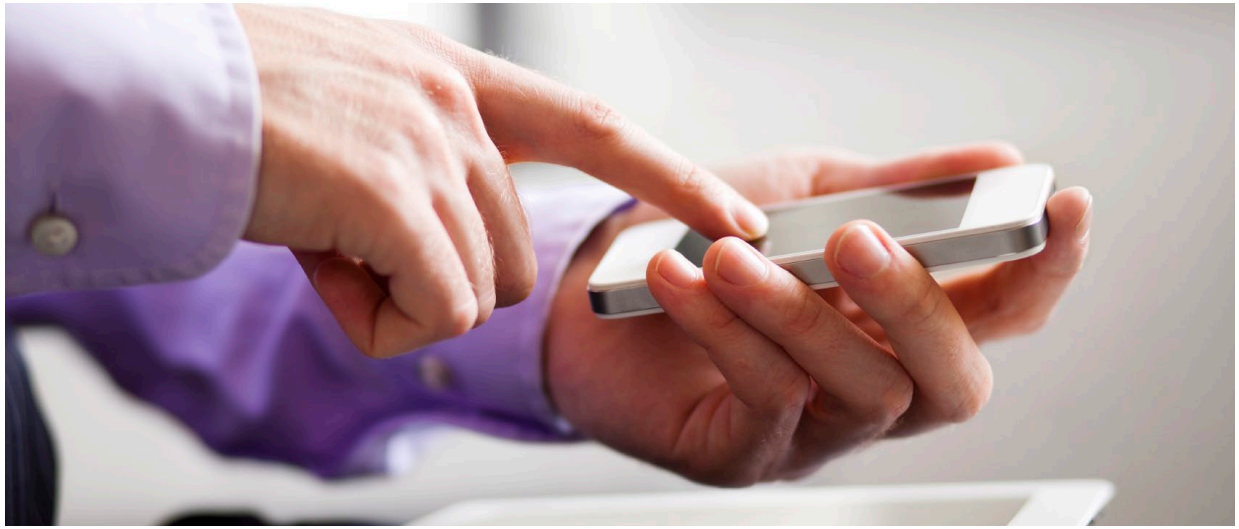
Financial institutions must thwart data theft attempts on a number of fronts, both internal and external, as data is moved globally and quickly across multiple IT infrastructures and stored in multiple repositories. One small breach can cause a great deal of damage. The Bring-Your-Own-Device (BYOD) phenomenon adds even more risk for customer information residing in financial institutions, so the challenge becomes balancing employee productivity and security.

Data breaches are very common thanks to aggressive attacks by cyber-criminals that use strategies such as sending malicious links contained in emails or social networks, bogus software updates or other requests that guide a financial institution's employees to websites that install malware.

Even exposing a small percentage of customer information can lead to the dire consequences for a financial institution, including the direct loss of funds, contravention of government regulations, serious fines or limitations placed on future business operations, while legal action could be launched by customers demanding compensation.

All of these scenarios damage the credibility of the financial institution that leads to lost business over time.

Regional and global legislation and regulations,provide great incentive for employing stringent data security in financial institutions. These laws provide clear guidance relating to the protection of customer information and the majority specifically mandate that sufficient and relevant technical and organizational measures be taken to secure personal data.



# EXECUTIVE SUMMARY

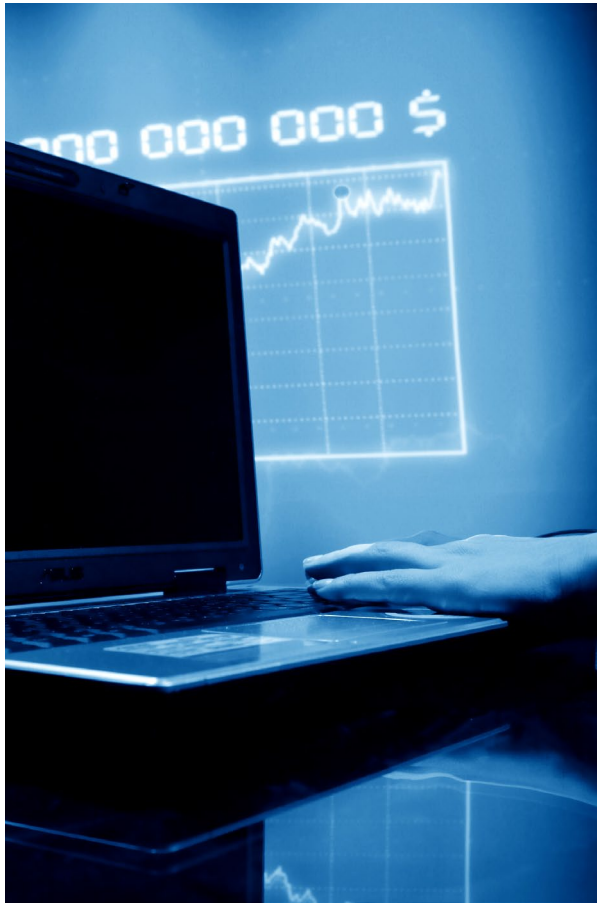
Data security analysts and experts within the banking and financial sectors, universally recommend the use of data encryption. It's the most effective way of achieving data security by requiring a password or key for data to be read by a recipient, and the best defense against data breaches begins with a well-thought out strategy for mitigating current and future risks.

Best practices combined with understanding regulations and legislation where a financial institution operates can help inform data security strategies. In addition to protecting their networks from intrusion, financial institutions should look to incorporate full disk encryption (FDE) and pre-boot network authentication (PBNA). Effective FDE solutions are designed with the heterogeneous IT environment in mind, and should be able to leverage existing network log-in credentials in addition to multi-factor authentication. PBNA enhances security through authentication at pre-boot rather than at the OS login. Users can still enjoy the simplicity of single password access. It provides a means for authenticating encrypted devices to the network before the OS ever loads.

Financial institutions tend to have hybrid security environments that include a combination of hardware and software encryption and multiple operating systems on a broad array of devices. FDE and PBNA when deployed correctly can provide the security necessary to safeguard customer information, and allow financial institutions to address compliance and regulatory issues at the same time.

Ultimately, securing sensitive data with the right technology based on best practices and the regulatory environment also leads to better business outcomes for the financial institution, and developing a reputation for no data breaches as compared to competitors ultimately reflects well on the company's bottom line.

# INTRODUCTION



When consumers provide their personal information to a company or government agency, there is an understood agreement that these entities will protect any personally identifying information (PII) they share, but while many organizations state they will in fact keep this PII in confidence, often their best practices and technology are not as stringent as required to keep this promise.

PII is generally defined as a person's name, Social Security (or Identity Card), driver's license or financial account number. Depending on the organization that stores this PII, expectations are higher. Healthcare is one sensitive area, but expectations of data security are especially high for financial institutions. As the number of data breaches and identity thefts rise in this sector, adopting a strong data security strategy is vitally important, both to protect credibility of the financial institution and to stem the associated costs of a publicized data breach.

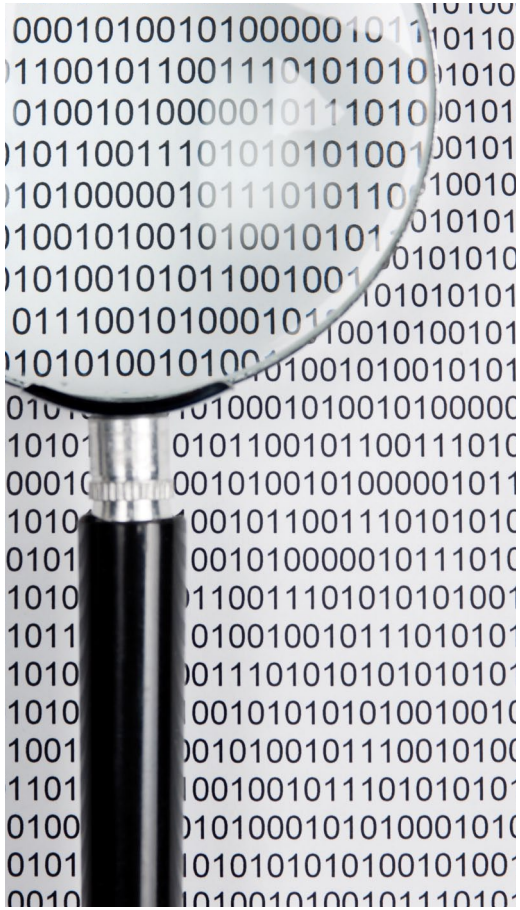
# THREATS ON ALL FRONTS

Financial institutions are obviously a popular target of criminal activity due to the monetary gain involved and hence they must aggressively combat data breach vulnerabilities, both internal and external.

Securing PII, especially electronic PII in a digital age, is becoming exponentially more challenging for financial institutions. Data is moved globally and quickly across multiple IT infrastructures – not just their own but across business stakeholder's infrastructure. Because PII moves so quickly, it can be hard to keep track of. In addition it can be duplicated into many repositories, sometimes unknowingly. It may be adequately protected in multiple databases and locations, but all it takes is a breach at one location to negatively affect customers and cause huge headaches for the institution.

In addition to multiple repositories, there are multiple devices accessing PII thanks to things like the Bring-Your-Own-Device (BYOD) phenomenon. Employees are using multiple devices to access customer data – laptops, smart phones and tablets – that often leave the secure, internal network of the financial institution. While this improves worker productivity, it also means data becomes even more vulnerable. Catching up on work in a coffee shop or airport is commonplace, but it often means a device is connected to a WiFi network that does not have stringent security. Even if the device never connects to an outside network, locally stored data can become compromised if the device is lost or stolen, or falls into the wrong hands.

Locking down devices so they can only access data within the financial institution is an option, even if it does hamper productivity, but even still these devices can fall prey to careless or disgruntled employees. In addition, there are individuals and groups actively attacking the networks of financial institutions.



# THREATS ON ALL FRONTS

Thousands of data breaches occur each year. The migration of financial transactions from paper-based systems to digital and online ones has led cyber-criminals to follow those transactions. These predators have begun to focus on targeting web sites with inadequate security protections in place with the goal of obtaining passwords and user names. Their strategies include using malicious links contained in emails or social networks, such as bogus software updates or other requests that guide a financial institution's employees to websites that install malware. Because of the common practice of using the same password for multiple accounts, if a hacker gains access to one online account, they can typically compromise several others.[i] In addition to the records of hundreds of thousands or millions of individuals, these attacks can compromise corporate and national assets.

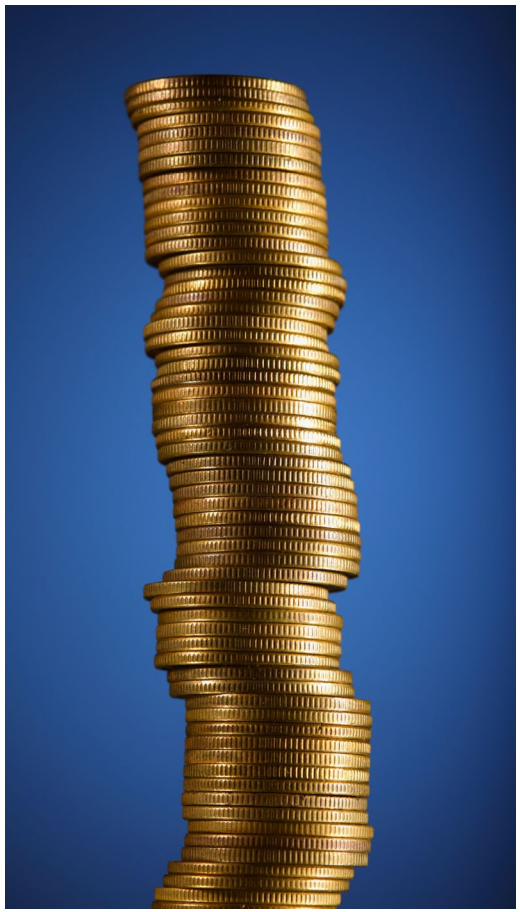
A 2012 study by Experian found that remote access was the biggest cause of data breach, accounting for 45 per cent of analyzed attacks.[ii] Meanwhile, KPMG's Data Loss Barometer report for the same year showed that financial services was one of the sectors most likely to experience a "data incident" and ranks as the fifth worst among industry performers.

In 2013, the Identity Theft Resource Center, which began tracking data breaches in 2005, found that hacking remained the number one cause (representing over one-fourth [25.8 percent]) of recorded breaches. Runners up included: subcontractors (or third-parties) 14.4 percent and data in transit (12.9 percent); insider theft, employee error and/or negligence, and accidental exposure, came in at 11.6, 9.2, and 7.6 percent, respectively. All told, the report found that 59.1 percent of U.S. publicly reported breaches compromised a total of 57 Million records in 2013 alone.[iii] The number of unreported or underreported breaches is believed to make this number substantially greater. Forty-seven percent of those records involved exposure of PII, specifically, Social Security numbers.

# ONE SMALL BREACH, BIG CONSEQUENCES

Financial institutions that don't do an adequate job of protecting PII are more likely to face dire consequences such as government fines by breaching regulations, direct and possible large financial losses, excessive legal fees as a result of claims from affected customers and a negative brand image

Just exposing a small percentage of customer PII can lead to the downfall of a financial institution depending on the customers affected and the amount of money involved. Obviously, there is the direct loss of funds which if significant enough, could mean the collapse of the organization. If the breach contravened a government regulation, there could be serious fines leveled against the institution and even limitations placed on future business operations. Legal action could be launched by customers demanding significant compensation. All of these scenarios damage the credibility of the financial institution that leads to lost business over time, and doing damage control can consume a great deal of financial and human capital and in turn has a negative impact on an organization's ability to run daily operations.



# LEGISLATION AS INCENTIVE FOR SECURITY

Legislation and regulations, whether regional or global, provide a great impetus for employing stringent data security in financial institutions.

In 2003, California became the first state in the U.S. to require data breach notification and has carried the distinction of having the strongest consumer privacy laws in the country ever since. In the intervening years, all but four U.S. states have adapted laws similar to California's, and U.S. federal regulation modeled upon California's laws is being proposed. The intention of the law's authors was to provide the earliest possible alert to consumers if they were at risk of identity theft. The 2012 Data Breach Report for California commissioned by the Office of the Attorney General (OAG) and produced by California's Department of Justice was conducted to gain a better understanding of what types of breaches were occurring, the vulnerabilities they could expose, and the best actions to aid in preventing future breaches.

The report covered California breaches across a broad number of sectors, including financial services, and the OAG made the following recommendations:

1. Encrypt digital personal information transmitted outside company networks. (As a strong signal of the weight this issue carries, the OAG is making investigation and enforcement of data breaches involving unencrypted personal information a priority and encouraging other law enforcement agencies to do the same).

2. Review and tighten security controls on personal information (provide regular trainings in organizational policies and procedures for employees and contractors).

3. Enact legislation that requires companies to unilaterally use encryption to protect personal information on portable devices (media and email) – the National Institute of Standards and Technology's standard approved for U.S. Government organizations (FIPS 197) might be an acceptable standard.

# UNDERSTANDING BEST PRACTICES

Data security analysts and experts within the banking and financial sectors, as well as a host of organizations such as the National Institute of Technology Standards (NIST), universally recommend the use of data encryption, which is the most effective way of achieving data security by requiring a password or key for data to be read by a recipient. The two main types of data encryption are asymmetric encryption, also known as public-key encryption, and symmetric encryption. Security experts have recommended financial institutions enable encryption for data at rest, in transit, and during processing to provide maximum data security and confidence for business partners and customers.

**THE BEST DEFENSE AGAINST DATA BREACHES BEGINS WITH A WELL-THOUGHT OUT STRATEGY FOR MITIGATING CURRENT AND FUTURE RISKS. TO START:**

1. Conduct a current data security risk assessment
2. Determine security gaps and create or update your organization's policy on data security
3. Train (or retrain) all employees that intersect PII on the most current data security threats (especially those linked to employee negligence) and safeguards for protecting PII.

> **"Security experts have recommended financial institutions enable encryption for data at rest, in transit, and during processing to provide maximum data security and confidence for business partners and customers."**

The FFIEC 2005 Guidance states, "The agencies consider single-factor authentication as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."[viii] Though seemingly self-evident, many of the breaches that occurred in the previous section did so because the FIs only required single-factor authentication.

**IN A SUPPLEMENT TO THIS (2011), THE FFIEC FURTHER RECOMMENDS THAT FIs UNDERTAKE:**

- Layered security for business financial accounts suitable to their inherent risks
- Annual risk assessments evaluating high-risk transactions
- Promote education for business and individual account holders
- Processes that detect abnormal account activity[ix]

# UNDERSTANDING BEST PRACTICES

## IN ADDITION TO THESE GENERAL GUIDELINES, DATA SECURITY EXPERTS RECOMMEND:

- Assessing where business is being conducted
- Knowing all applicable rules, especially for international locations
- Knowing what needs to be encrypted by the appropriate data type (an "encrypt everything that moves" strategy is suboptimal – work with legal counsel to determine this)
- Understanding applicable data formats
- Identifying data at rest in, 1) databases, 2) file shares and storage (e.g. Storage Area Network – or SAN), and 3) email systems, 4) desktops, laptops, PDAs, Smartphones and removable storage devices, back up media, and end-of-life devices.
- Locating data "in flight"
  - Assessing the path of PII (either by sniffers or network traffic capture/monitor software, determine if PII is being transmitted with or without proper encryption)
  - Determining which network devices are storing PII or related information, and
  - Inspecting gateway devices (e.g., mail servers and proxies)
- Encrypting or obfuscating any PII located
- Finding a reputable data security partner to continually monitor and implement the most appropriate best practices for current and emerging data security threats, and lastly,
- Creating a manageable encryption policy (or policies), which should include:
  - Strong encryption (128-bit keys or larger)
  - Testing
  - Auditing of a sample of systems post-roll out
  - Role-based controls (e.g., HR cannot read/access R&D data, etc.)
  - Robust key management processes
  - Routine and ongoing audits of all operations to ensure data security and encryption policies are alive and well *in practice*

# ESSENTIAL TOOLS AND TECHNOLOGIES

These best practices combined with understanding regulations and legislation where a financial institution operates can help define data security strategies. In addition to protecting their networks from intrusion, they should look to incorporate two key technologies to protect PII: full disk encryption (FDE) and pre-boot network authentication (PBNA). FDE is encryption at the hardware level and works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the authentication key to decipher the data. Without that key, the data remains inaccessible. FDE is becoming standard practice in the enterprise organizations, including financial institutions. PBNA adds another level of security by requiring authentication at pre-boot rather than at the OS login improving policy protection by making it easy for administrators to push system updates or quickly assign or withdraw privileges from users.

While passwords, biometrics, smart cards and other tokens do offer a high level of security, they aren't infallible; they can be cracked, thereby exposing sensitive business data. The challenge faced by IT departments is how to keep costs low, while ensuring IT administrators are efficient and end user experiences are unaffected. The larger the organization and the more platforms in use, the greater the need for FDE. In fact, FDE should be deployed on every device regardless of platform for full data security. It only takes one stolen laptop to have not been properly secured and encrypted to make all of your FDE efforts irrelevant and expose PII.

Effective FDE solutions are designed with the heterogeneous IT environment in mind, and should be able to leverage existing network log-in credentials (instead of only a PIN) in addition to multi-factor authentication, including UPEK fingerprint readers, smart cards, USB tokens, trusted platform modules and CAC/PIV cards. This provides the ability to lock down system access and guarantee high-level security of devices. A multi-factor authentication approach is critical for any financial institution.

# ESSENTIAL TOOLS AND TECHNOLOGIES

Meanwhile, PBNA increases and enhances security through authentication at pre-boot rather than at the OS login. Users can still enjoy the simplicity of single password access. It provides a means for authenticating encrypted devices to the network before the OS ever loads. Before any data on a device is decrypted and a user granted access, the user must input their credentials in the form of a password that is verified by a network connected server and then allow the user to log-on to a device and start the operating system (OS) log-in process. It means data is never exposed until the user credentials are verified before the standard OS log-in process.

At the same time, PBNA allows financial institutions to manage groups and really control how, what, when and where users access information via policy controls.

Given their size and long histories, financial institutions have hybrid security environments that include a combination of hardware and software encryption and multiple operating systems on a broad array of devices. FDE and PBNA when deployed correctly can provide the security necessary to safeguard PII, and allow financial institutions to address compliance and regulatory issues at the same time. This can all be achieved without negatively affecting existing processes and being transparent to the users. The end result is increased security and lower IT costs.

## WHAT CAN DATA ENCRYPTION DO FOR MY INSTITUTION?

Ultimately, securing PII with the right technology based on best practices and the regulatory environment also leads to better business outcomes for the financial institution. Developing a reputation for no data breaches as compared to competitors ultimately reflects well on the company's bottom line: existing customers remain loyal while new customers flock to a financial institution where they know their PII is secure. Financial institutions that are successful with data security measures generally enjoy greater public and shareholder confidence, and in some instances, government protection from wide-spread liability.

i. Javelin Strategy & Research, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters" (February 2013), www.javelinstrategy.com, reported that data breach victims were 22 .5 percent likely to experience identity fraud, over four times greater than the general public.
ii. http://www.experian.com/blogs/data-breach/2013/03/26/data-breach-numbers-are-up-worldwide/
iii. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html
iv. http://www.globalknowledge.ca/training/whitepaperdetail.asp?pageid=644&wpid=1183&country=Canada
v. http://en.wikipedia.org/wiki/Data_Protection_Act_1998
vi. http://en.wikipedia.org/wiki/Data_Protection_Directive
vii. http://www.unisys.com/unisys/news/detail.jsp?id=1120000970027910151
viii. https://www.ffiec.gov/pdf/authentication_guidance.pdf
ix. http://www.globalknowledge.ca/training/whitepaperdetail.asp?pageid=644&wpid=1183&country=Canada

# READY TO LEARN MORE?

WinMagic provides the world's most secure, manageable and easy-to-use data encryption solutions. With a full complement of professional and customer services, WinMagic supports over five million SecureDoc users in approximately 84 countries. We can protect you too.

For more information on SecureDoc Enterprise Server contact **sales@winmagic.com** or visit our website to access a number of valuable resources:

**PRODUCT PAGE**
**http://www.winmagic.com/products**

**WHITE PAPERS**
**http://www.winmagic.com/resource-centre/white-papers**

## CONTACT

**WinMagic Inc.**
Phone: 905. 502. 7000
Fax: 905. 502. 7001

Toll Free: 888. 879. 5879

**sales@winmagic.com**
**www.winmagic.com**

## SOCIAL MEDIA


http://blog.winmagic.com/


http://www.facebook.com/WinMagicInc


http://www.linkedin.com/company/winmagic


http://twitter.com/winmagic

http://www.youtube.com/user/winmagicinc

## WANT TO TRY OUR SOFTWARE?

**Click here to request a free evaluation** ›