

# In Your Best Interest

## To protect yourself from a data/compliance breach

We are providing the below guidelines which can help protect your company from a breach; which could result in lost revenue, expensive legal fight or restriction of your company to obtain credit reports from the 3 national repositories. The three national credit bureaus are very strict in **requiring each User of their credit reports to implement security procedures to avoid a data/compliance breach.**

### Security Access Control Measures

- Do not provide your account code or password to anyone.
- Develop strong Alpha Numeric passwords. Don't use your name, company name, address.
- Each User in your office should have their own User ID and Password.
- If an employee leaves your company, disable their User ID and Password immediately.
- Implement password protected screensavers (5 minute timeout) to protect unattended workstations.
- Establish procedures for responding to security violations and theft of laptops.
- Do not access your own credit report or those reports for family, friend(s) unless it is in connection with a credit transaction under permissible purpose guidelines.
- After normal business hours, turn off and lock all devices used to obtain credit information.
- Keep all paper documents with consumer information in a secure, locked environment when not in use. Do not leave such documents on your desk overnight.
- All desktops/laptops should be password protected to further protect credit reports and consumer ID
- Develop Security Violation Procedures which should include 1) notifying the credit bureau of the security violation. 2) notification to the consumers whose data may have been breached. 3) providing each consumer with a credit bureau monitoring service
- Implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records in accordance with FACTA Disposal Rules.
- Keep your laptops in a secure place. Do not leave unattended. Password protects all documents containing consumer ID information.

## Borrowers' Authorization

- You are required to obtain the borrower's authorization **prior** to obtaining a credit report.
- This authorization must be maintained for **3 yrs** for consumer disputes or audits.
- If verbal, use a form that documents their approval, e.g. city of birth or date of birth.
- If over the internet, print the acceptance page.
- Use the consumer's credit card to pay for the report. This will not only save you money, there will be no question that they gave approval.
- If using consumer's credit card, check the credit report to make sure the credit card is shown on the report.
- Never mail or fax a credit report to a consumer unless you have met with them and verified their identity.
- Before emailing a credit report, be sure you have encryption software for security of the consumer's information.

## Protecting your system data

- Protect internet connections with dedicated, industry recognized Firewalls.
- Internal IP addresses must not be publicly accessible. Network address translation (NAT) technology should be used.
- Any stand alone computers that directly access the internet must have a desktop Firewall.
- Encrypt Wireless access points with a minimum of WEP 128 bit encryption. WPA encryption where available.
- Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points
- Keep operating system(s), Firewalls, Routers, servers, personal computers (laptops and desktops) current with appropriate system patches and updates.
- Implement on a weekly basis the use of a current, commercially available Computer Virus detection, scanning product on all computers, systems, and networks. Keep the anti-virus software up-to-date.
- Implement on a weekly basis the use of a current, commercially available anti-Spyware scanning product on all computers, systems, and networks. Keep anti-Spyware software up-to-date.

*The above guidelines are not intended to be a complete data/compliance breach guide. For complete compliance, you should obtain and follow all the federal regulations concerning protecting consumer identification information.*