



Deterring Identity Theft

CHALLENGES AND OPPORTUNITIES FOR FINANCIAL INSTITUTIONS

The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year.

Identity theft complaints increased 22 percent from 2007 to 2008 (Javelin 2009 Identity Fraud Survey Report)

The average consumer costs of identity fraud were \$496 per incident in 2008 (Javelin 2009 Identity Fraud Survey Report)

Industry estimates put the total cost of identity fraud at \$48 billion in 2008 (2009 Javelin Strategy & Research)

Maintaining customer trust is especially important in the financial services sector. Direct monetary loss is not the only way in which a financial institution can be affected by identity theft. It can also be impacted financially if personal information entrusted to it by customers or employees is stolen or inadvertently lost. A security breach can also damage a financial institution's reputation and erode trust in its commitment and ability to protect sensitive information.

Identity theft has been the top consumer complaint in recent years. Identity theft in financial crimes creates two victims. The first victim is the unfortunate consumer or business whose information has been co-opted. The second victim is the financial institution, merchant, government agency or other creditor that suffers the monetary loss when the information is misused.

› Identity Theft Prevention Tips

The fact that financial institutions are also employers introduces another set of challenges. Employee records are a lucrative source of data for identity thieves. Employee and applicant information may be accessed and misused while it is being acquired, validated, stored, transmitted or destroyed.



deter

To overcome these challenges, financial institutions can take the following steps to strengthen customer and employee relationships:

CUSTOMER	EMPLOYEE:
Introduce 'secure account' bundled with fraud protection services	Offer an identity theft prevention product to staff as an employment benefit
Create awareness of your identity theft prevention policies with direct marketing, statement inserts and check package inserts	Reward employees for preventing fraud and loss
Provide complimentary credit monitoring in the event of a data breach	Ensure all employees who handle customer information have an understanding of identity theft
Earn account holder loyalty by arming them with current information to help them prevent, detect and mitigate identity theft	Educate employees using training sessions, posters, handouts and other tools

- Position work stations and computer screens so personal information cannot be seen by employees or customers who may randomly be in the vicinity.
- Ensure all computers are logged off and all personal information is properly secured after hours. Information stored on laptops should be password protected and encrypted.
- Temporary employees and contractors with access to employee and/or customer information should be subject to screening and trained in security practices and expectations.
- Collect and retain only essential data on employees and applicants.
- Determine all places where employee and customer personal information is found, how long it is retained and who has access. Verify the information is securely stored and used, with access granted on a need-to-know basis.
- Communicate regulatory requirements (e.g. GLB, FACTA, SOX, PATRIOT) to customers and employees in clear terms.

› Security Awareness Reminders

- Designate knowledgeable individuals at each financial institution location to be focal points for customer service issues relating to identity theft crimes.
- Ensure all employees who handle customer information and/or deal with the public have a basic understanding of identity theft. This includes measures to detect, prevent and mitigate identity theft, as well as anti-fraud initiatives.
- Many financial institutions use SSNs to authenticate customers who call in. Use something other than SSNs or easily obtained personal data as phone gateway passwords.



- Periodically confirm document destruction practices. Discarded documents and magnetic media containing employee or customer data should be shredded or otherwise properly destroyed.
- Ensure hard drives have been destroyed, degaussed or scrubbed and all documents have been removed before selling or discarding used computers, file cabinets and other office equipment.
- Establish procedures for handling and resolving customer disputes concerning the accuracy of credit bureau reports.
- Establish security breach procedures.
- Establish processes for alerting customers if unusual or suspicious activity occurs on their account.
- Establish procedures for customers or employees called to active military duty to place a military flag on their credit bureau records.
- If a checking account is closed for fraud, confirm any valid outstanding checks written by the customer will be honored.

Additional Resources:

www.ftc.gov/idtheft • www.ftc.gov/infosecurity • www.OnGuardOnline.gov