Identity Theft Prevention: Tips for Businesses

We know your customers are important to you. Protecting their personal information from identity thieves is not only good business, but it's the law. To help you do right by your customers and comply with federal, state and local laws requiring you to protect their personal information, the New York City Department of Consumer Affairs (DCA) offers this legislative and best practices overview. Failure to comply may violate New York City's Consumer Protection and Licensing laws.

Know the Law

Identity Theft Prevention Programs. Effective November 2009, financial institutions and creditors must have put into operation written "identity theft prevention programs." Programs must detail how financial institutions and creditors will identify, detect, and respond to patterns, practices or specific activities—known as "red flags"—that could indicate identity theft. For more information, see:

- Fair and Accurate Credit Transactions (FACT) Act of 2003, Red Flags Rule: 16 CFR 681.2

Records Disposal. Paper and digital records containing customer information must be disposed of properly. Shredding is an acceptable method for paper records. Use "wipe utility" software to delete computer data permanently—simple deletion is not enough when recycling computers. For more information, see:

- New York City Administrative Code § 20-117 (g)
- New York State General Business Law Article 26 § 399-H (Section GBS)
- Federal Trade Commission Disposal Rule, 16 CFR Part 682

Security Breaches. If you become aware that an unauthorized party has accessed your customers' information, you are required to alert affected consumers and the appropriate authorities, including DCA. For more information, see:

- New York City Administrative Code § 20-117
- New York State Information Security Breach and Information Act, New York State Technology Law § 208 (Section STT)

Privacy Policy. All financial institutions must create and disclose their privacy policies to customers. The law defines "financial institutions" broadly to encompass companies that offer financial products or services to individuals like loans, financial or investment advice, or insurance. This also includes businesses that directly carry out any financial transaction (like banks) or help facilitate transactions, such as processing money orders, check cashing, brokering loans (like used auto dealers, furniture stores, etc.), debt collectors, tax preparers, and more. For more information, see:

- Gramm-Leach-Bliley (GLB) Act
- Federal Trade Commission Safeguards Rule, 15 U.S.C. § 6801-6809

Receipts. All businesses that accept payment by credit card must remove the expiration date and all but the last five digits of the credit card number from customer receipts. For more information, see:

- Fair Credit Reporting Act (FCRA) § 605 (g)
- New York State General Business Law Article 29-A § 520-a (Section GBS)

Best Practices

Security Protocols. Review how your business protects customer information—i.e., where information is stored and who has access to it—and change protocols as necessary to increase security. Train employees so they know the company's privacy policy and how to protect customers' personal information.

Ask for ID. Employees should ask for identification when customers pay by credit card. If employees are suspicious of a transaction and think the card may be stolen, they should call the store's credit card processing service and report a "Code 10." This phrase unobtrusively alerts the credit card company of potential identity theft activity.

Collect Less Information. Only collect the information necessary to complete the transaction and store it only as long as needed. The less customer information you store, the less you have to protect.

Restrict Access. Make sure documents that contain customers' identifying information, such as applications or merchant copies of credit card receipts, are not in sight of employees or the public, or otherwise accessible. A locked storage space can offer good protection.

Safeguard Computers. Install antivirus and firewall software on computers and regularly update it. Make sure that password-protected screen savers turn on once a computer is idle.

Stay Current with Online Security Measures. Your technology manager should remain aware of new issues or areas of concern in online security. Check with the Federal Trade Commission at **ftc.gov** for recommended resources about technology updates. Use the Federal Communications Commission's Small Biz Cyber planner at **fcc.gov/cyberplanner** to create a custom cyber security plan for your company.

NYC
Consumer Affairs

Bill de Blasio
Mayor

Lorelei Salas
Commissioner

For more information, visit nyc.gov/consumers. For information about the federal and state laws referenced here, please contact the organizations mentioned.