Korean

신원 도용 방지: 기업을 위한 정보

고객이 중요하다는 것은 당연합니다. 고객의 개인 정보를 신원 도용으로부터 보호하는 것은 올바른 일일 뿐만 아니라 법적 의무입니다. 뉴욕시 소비자사안부(DCA)는 기업이 고객을 위해 올바른 일을 하고 연방정부, 주정부, 지역정부의 고객 개인 정보 보호법을 준수할 수 있도록 본 법률 개요와 모범 사례를 소개해 드리고자 합니다. 준수하지 않을 경우 뉴욕시 소비자 보호 및 허가법에 위반될 수 있습니다.

법 알기

신원 도용 방지 프로그램. 2009년 11월부터 금융기관과 대출기관은 서면으로 된 "신원 도용 방지 프로그램"을 시행해야 합니다.프로그램은 금융기관과 대출기관이 어떠한 방법으로 신원 도용을 의미할 수 있는 성향, 관행 또는 구체적인 활동(레드 플래그)을 파악하고 감지하며 이에 대응할지를 상세히 규정해야 합니다. 자세한 내용은 다음을 참조해 주십시오.

- Fair and Accurate Credit Transactions, FACT, Act of 2003 (공정 및 정확 신용 거래법), 레드 플래그 규정: 16 CFR 681.2

기록 폐기. 고객 정보를 포함하고 있는 서류 및 디지털 기록은 올바른 방법으로 폐기되어야 합니다. 파쇄는 서류 기록에서 인정되는 방법입니다. “wipe utility” 소프트웨어를 사용하여 컴퓨터 데이터를 영구적으로 삭제해야 합니다. 단순한 삭제는 (컴퓨터 재활용 시) 충분하지 않습니다. 자세한 내용은은 다음을 참조해 주십시오.

- New York City Administrative Code (뉴욕시 행정법) § 20-117 (g)
- New York State General Business Law (뉴욕주 일반사업법) Article 26 § 399-H (섹션 GBS)
- Federal Trade Commission Disposal Rule (연방거래위원회 폐기규정), 16 CFR Part 682

보안 위반. 권한이 없는 사람이 고객 정보에 접근했다는 사실을 인식한 경우, 영향을 받은 고객과 DCA 등 해당 당국에 이 사실을 알려야 합니다. 자세한 내용은은 다음을 참조해 주십시오.

- New York City Administrative Code (뉴욕시 행정법) § 20-117
- New York State Information Security Breach and Information Act (뉴욕주 정보 보안 위반 및 정보법), New York State Technology Law (뉴욕주 기술법) § 208 (섹션 STT)

개인 정보 보호 정책. 모든 금융기관은 기관의 개인 정보 보호 정책을 세우고 이를 고객에 공개해야 합니다. 법률상 "금융기관"의 폭넓은 정의는 대출, 재정 자문, 투자 자문, 보험과 같은 금융 상품이나 서비스를 개인에게 제공하는 회사입니다. 여기에는 금융 거래를 직접 수행하는 기업(은행)과 우편환 처리, 수표 현금화, 대출 브로커(중고차 대리점, 가구 매장 등), 채무 추심, 세금 준비자 등 거래에 도움을 주는 회사들도 포함됩니다. 자세한 내용은은 다음을 참조해 주십시오.

- Gramm-Leach-Bliley (GLB) Act (그램–리치–브릴리법)
- Federal Trade Commission Safeguards Rule (연방거래위원회 보호규정), 15 U.S.C. § 6801-6809

영수증. 신용카드 결제를 수행하는 모든 기업은 고객 영수증에서 신용카드의 만료일과 마지막 5자리 번호를 반드시 삭제해야 합니다. 자세한 내용은은 다음을 참조해 주십시오.

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

모범 사례

보안 프로토콜. 소속 기업의 고객 정보 보호 방법(예: 정보 보관 위치, 정보 접근 가능자 등)을 검토한 후 보안 수준을 높이기 위해 필요하다면 프로토콜을 변경해야 합니다. 직원들이 회사의 개인 정보 보호 정책과 고객의 개인 정보 보호 방법을 알 수 있도록 직원을 교육하십시오.

신분증 요청. 직원들은 고객이 신용카드로 결제를 할 때 신분증을 요청해야 합니다. 거래가 의심스럽고 카드가 도난된 카드라고 판단되면, 직원들은 해당 매장의 신용카드 처리서비스 업체에 알리거나 "코드 10"을 신고해야 합니다. 이는 신용카드 회사에 신원 도용 가능성을 암묵적으로 알리는 표현입니다.

최소한의 정보 수집. 거래 완료에 필요한 정보만을 수집하고 필요한 기간 동안만 저장하십시오. 저장해야 할 고객 정보가 적을 수록 보호해야 할 대상이 적어집니다.

접근 제한. 신청서, 신용카드 영수증의 매장용 사본 등 고객 식별 정보가 포함된 서류가 직원들이나 일반인의 시선이 닿는 곳이나 접근 가능한 곳에 있지 않도록 하십시오. 잠긴 보관 공간에 두면 효과적으로 보호할 수 있습니다.

컴퓨터 보호. 바이러스 백신 및 방화벽 소프트웨어를 컴퓨터에 설치하고 주기적으로 업데이트하십시오. 컴퓨터가 유휴 상태가 되면 비밀번호로 보호된 화면보호기가 켜지도록 설정하십시오.

최신 온라인 보안 방침 준수. 기술 관리자는 온라인 보안 사안의 새로운 문제나 분야에 대해 알고 있어야 합니다. 연방거래위원회**(ftc.gov)**에서 기술 업데이트에 대한 추천 자료를 확인해 보시기 바랍니다. 연방 커뮤니케이션 위원회의 소기업 사이버 플래너**(fcc.gov/cyberplanner)**를 이용하여 회사에 적합한 사이버 보안 플랜을 수립하십시오.

NYC
Consumer Affairs

Bill de Blasio
Mayor

Lorelei Salas
Commissioner

자세한 내용은 nyc.gov/consumers를 참조해 주십시오.
여기에 명시된 연방법 및 주법에 대한 자세한 내용은 언급된 기관으로 문의하시기 바랍니다.