It's 2014: You Will Be Hacked

The Executive Roundtable Series
June 25, 2014 | No. 3

Christopher G. Smith
csmith@smithlaw.com

SMITH ANDERSON

It's 2014: You Will Be Hacked!

Smith Anderson Presents

SafeguardingBusiness.com…

Your Resource for Safeguarding Critical Business Information

Companies seeking a competitive advantage in the battle to keep their innovations and information secure in today's world of data breaches have a sophisticated ally in Smith Anderson.

NON-COMPETE AND TRADE SECRETS

DATA USE, PRIVACY AND SECURITY

INTELLECTUAL PROPERTY

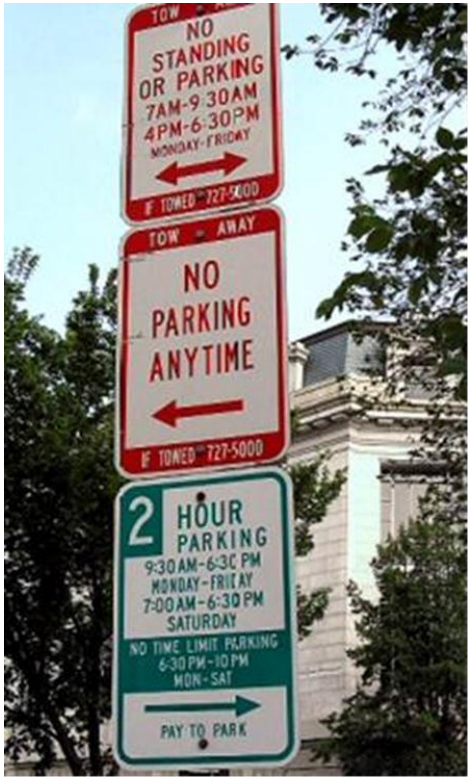
Our people have the experience, insights and firepower to help safeguard your business.

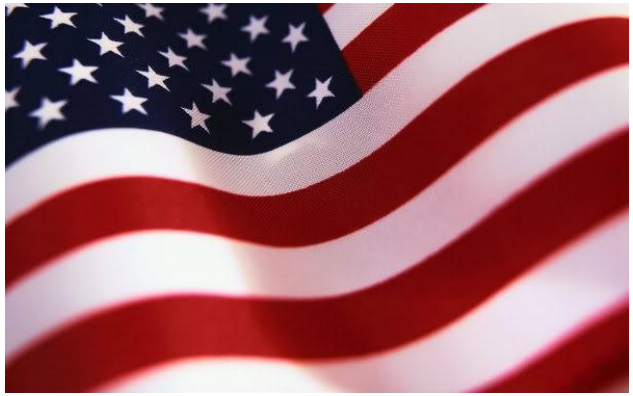
SMITH ANDERSON

Overview

- Complexity
- Risks
- “Security Breach”
- Response
- Prevention

Complexity


NO
STANDING
OR PARKING
7AM-9:30AM
4PM-6:30PM
MONDAY-FRIDAY
TOW - AWAY
NO
PARKING
ANYTIME
IF TOWED 727-5000
2 HOUR
PARKING
9:30 AM-6:30 PM
MONDAY-FRIDAY
7:00 AM-6:30 PM
SATURDAY
NO TIME LIMIT PARKING
6:30 PM-10 PM
MON-SAT
PAY TO PARK




N★C
APRIL 12th 1776

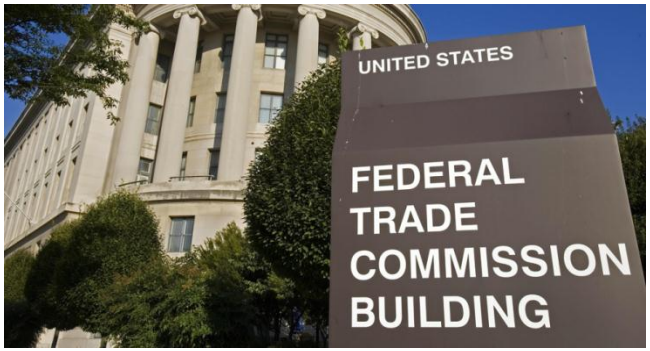
Complexity–Contracts

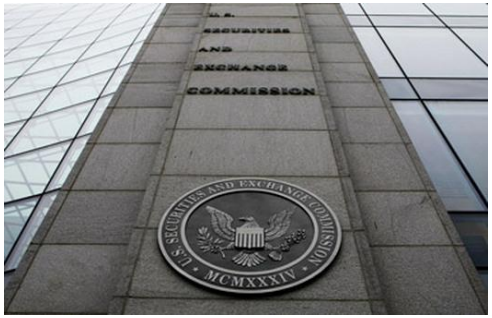
Notification of Security Breach. In addition to any other provisions of this Privacy Statement, Supplier shall notify Company immediately upon discovery or notification of any actual, po
Da
de
ide
the
oth
in
breach, and to carry out any recovery necessary to remedy the impact. Supplier also agrees to bear any cost or loss Company may incur as a result of the breach, including without limitation, the cost of notifying individuals if Company determines to do so.

In addition to any other provisions of this Privacy Statement, Supplier shall notify Company immediately upon discovery or notification of any actual, potential or threatened security breach (i.e., unauthorized access or use) involving any Company Data and/or Personal Information.

Risks

- Government enforcement
  - FTC
  - SEC
  - State





Risks

- Damages claims by individuals/class actions
- Shareholder derivative actions

WHAT'S A "SECURITY BREACH"

SMITH ANDERSON

WHAT'S A "SECURITY BREACH"

- North Carolina Identity Theft Protection Act, NCGS 75-60 et. Seq.

(14) "Security breach". — An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

WHAT'S A "SECURITY BREACH"

- North Carolina Identity Theft Pro

- unauthorized access *and*
- acquisition
- of PII *and*
- illegal use
  - has occurred *or*
  - is reasonably likely to occur *or*
- *or* that creates material risk of harm to the consumer

(14) "Securi
acquisit
persona
has occ
risk of h
acquisit
tion al
security
employ
security
a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

Question 1

- Is there a “Security Breach” if there is unauthorized access to your system, but no acquisition of PII?

a. Yes
b. No
c. Maybe
d. I have no idea

WHAT'S A "SECURITY BREACH"

- North Carolina Identity Theft Protection Act, NCGS 75-60 et. Seq.

(14) "Security brea
acquisition of u
personal inform
has occurred or
risk of harm to
acquisition of e
tion along wit
security breach
employee or ag
security breach
a purpose othe
subject to further unauthorized disclosure.

- unauthorized access *and*
- acquisition
- of PII *and*
- illegal use
  - has occurred *or*
  - is reasonably likely to occur *or*
- *or* that creates material risk of harm to the consumer

Question 2

- Same question. Does the NC Attorney General think there was a "Security Breach" under NC law?

a. Yes
b. No
c. Maybe
d. I have no idea

Question 3

- What if documents, including PII of ***customers*** are left in a dumpster for a week, and then retrieved intact by an employee?

a. Yes
b. No
c. Maybe
d. I have no idea

Question 4

- What if documents, including PII of ***employees*** are left in a dumpster for a week, and then retrieved intact by an employee?

a. Yes
b. No
c. Maybe
d. I have no idea

Question 5

- According to the Ponemon Institute, in 2013, what was the average, per-lost-record cost in the Healthcare industry of responding to a data breach?

$_____

Response

- Counsel
- Forensic investigation

Prevention

- The right paper
  - Risk allocation in private contracts
  - Arbitration provisions
  - Insurance

Prevention

Prevention

- The right culture
  - Target as a case study
  - Assign ownership of the issue
  - Training
  - Response team

It's 2014: You Will Be Hacked

The Business Roundtable Series 2014, No. 3

Alicia A. Gilleskie, agilleskie@smithlaw.com

Practice Group Leader, Data Use, Privacy and Security Practice Group

Jackson W. Moore, jmoore@smithlaw.com

Christopher G. Smith, csmith@smithlaw.com

SMITH ANDERSON

Data Breach Checklist

At Smith Anderson, our Data Use, Privacy and Security team helps clients protect, manage, defend and leverage the digital technology assets that are core to their business. Our expertise merges regulatory compliance, technology law and licensing, commercial contracting and dispute management, yielding our unique ability to advise clients on all aspects of data. Several of our team members are former in-house counsel, which gives us firsthand experience of our clients' perspectives.

Pre-Breach Planning

- Implement appropriate technical, administrative and physical security safeguards
- Prepare and maintain data privacy and security policies and procedures
- Designate a privacy officer and a security officer
- Prepare and implement a data breach response policy
- Identify data sources, inventory sensitive data and map locations
- Assemble a data incident response team and applicable roles
- Outline critical steps to take within the first 24 hours of a suspected breach
- Train staff to identify and report suspected breaches
- Implement a self-audit plan, to include data security and compliance assessments
- Develop and maintain data privacy and security standards for third party service providers
- Establish relationships with outside advisors who are knowledgeable about data breaches (*e.g.,* IT, forensics and counsel)
- Restrict access to information on a "need to know" and "minimum necessary" basis
- Track data breach laws, rules and notification mandates
- Consider adequacy of network security levels and encryption of sensitive data
- Follow a data retention policy with a plan to destroy or dispose of unneeded data

Post-Breach Efforts

- Assess gaps and evaluate effectiveness of current policies and procedures
- Update technology controls and policies and procedures
- Revisit privacy, security and response plans and make appropriate changes
- Conduct retraining of appropriate personnel
- Maintain a breach report in accordance with regulatory requirements
- Focus on monitoring crisis communications and restoring customer relations

Your Data Breach Response Team Stakeholders

Forensics | Legal | Security Contacts – Infrastructure and Physical
Information Technology | Privacy Officer | Security Officer | Human Resources
Internal Auditors | Management | Corporate Communications/Public Relations

Data Breach Response

- Engage outside forensic and IT advisors immediately
- Confirm breach has ended and lock-down of systems (*e.g.*, change passwords and encryption keys)
- Isolate and preserve compromised systems and data
- Investigate scope of breach to determine types of information compromised and number of affected individuals
- Determine whether access to networks or systems can be ruled out by IT and forensics
- Attempt to retrieve lost or otherwise compromised data
- Identify notification timeframes and requirements
- Document your work, but coordinate with counsel on preparation and treatment of written materials related to the breach
- Act swiftly, as regulatory timeframes begin upon discovery of the breach
- Consider notifying law enforcement
- Involve counsel to analyze legal obligations
- Develop and deliver notices to affected individuals and agencies in accordance with regulatory mandates and timeframes
- Evaluate the need for a toll-free number for affected individuals to receive specific information and assistance
- Consider offering credit monitoring, identity repair services, or identity theft insurance for affected individuals
- Cooperate with regulatory and governmental inquiries

Data Use, Privacy and Security Practice Group
www.SmithLaw.com/privacy
Practice Contact: Alicia Gilleskie — 919.821.6741, agilleskie@smithlaw.com
Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

SMITH ANDERSON

SMITH ANDERSON

Safeguarding Business

May 21, 2014

MORE INFORMATION

IF YOU HAVE QUESTIONS ABOUT THIS CLIENT ALERT, PLEASE CONTACT:

Jackson Moore
919.821.6688
jmoore@smithlaw.com

Alicia Gilleskie
919.821.6741
agilleskie@smithlaw.com

Christopher Smith
919.821.6745
csmith@smithlaw.com

Lauren Bradley
919.821.6648
lbradley@smithlaw.com

PRACTICE AREAS

Data Use, Privacy and Security

Government Contracting

Technology

Will the Cybersecurity Framework Create a New Standard Operating Procedure for Businesses?

On February 12, 2013, President Barack Obama issued Executive Order 13636 (EO 13636) entitled "Improving Critical Infrastructure Cybersecurity." [1] EO 13636 noted the importance of cybersecurity for the nation's security and economy and directed the National Institute of Standards and Technology (NIST) to create the **Cybersecurity Framework** (the Framework) for critical infrastructure.[2] On February 12, 2014, NIST released the Framework.[3] The Framework is the result of a public-private collaboration with 3,000 individuals and organizations rather than the creation of Washington regulators.[4] The Framework is essentially a guidebook of risk-based principles and practices for all businesses to manage cybersecurity threats. It is not unique to critical infrastructure industries.

At the present time compliance with the Framework is not required, as the Framework is not an act of Congress. Also, EO 13636 directed NIST to create the Framework expressly for critical infrastructure. However, the Framework could be applied by *any* organization. The Framework has three parts to assist organizations in managing cybersecurity risks: the Framework Core, the Framework Profile and the Framework Implementation Tiers.[5] Together, they provide a strategic way to identify activities and outcomes, create goals and measure progress. The Framework is intended to be flexible and molded to suit organizations of a variety of sizes and from a variety of industries.

While voluntary, businesses should pay attention to the Framework, even those outside of "critical infrastructure." There are at least three reasons to be mindful of the Framework:

1. EO 13636 called for various federal government agencies to provide incentives to companies using the Framework. Currently, the United States Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, is providing non-monetary incentives, including guidance on how to implement the Framework.[6] Other incentives, including monetary ones, are being considered and could become available.[7]

2. The Framework provides a "best practices" roadmap for cybersecurity. As such, it might be used as evidence in court of what a company *should have done* prior to a cybersecurity or data breach. Because the Framework is not a "one size fits all" solution, there are theoretically

best practices that could apply to any company. Failure to implement the Framework could be used as evidence of fault in the event of a cybersecurity incident.[8]

3. Although the Framework is currently voluntary, in the future federal and state governments could link compliance with the Framework to grants, contracts and regulated industries. In the private sector, insurance companies might tie premiums to compliance with the Framework.[9] Thus, the Framework may become mandatory in practice, even if legally voluntary.

Cybersecurity threats are on the rise. Companies of any size and from any sector could be the next target. The Framework should be reviewed and considered carefully by any company that holds data. The availability and flexibility of the Framework lends itself to being applied if there is a government investigation or litigation arising out of a data breach. Aside from the potential use in litigation, implementation of the Framework could put your company ahead of the curve to receive potential incentives and if the Framework becomes mandatory in practice.

[1] Exec. Order No. 13,636, 78 Fed. Reg. 33 (Feb. 19, 2013).

[2] *Id.* §§ 1, 7.

[3] Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity.

[4] Wyatt Kash, *Why Businesses Can't Ignore US Cybersecurity Framework*, Info. Week (Feb. 14, 2014).

[5] Framework, *supra* note 3, at 1, 7-12.

[6] *Critical Infrastructure Cyber Community Voluntary Program*, US-Cert, (last visited April 15, 2014).

[7] Chris Strohm, *Obama Cybersecurity Plan Seen Lacking Perks for Business*, Bloomberg (Feb. 11, 2014),

[8] Kash, *supra* note 4.

[9] Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, The White House Blog (Aug. 6, 2013, 11:04 AM).

SUPREME COURT OF THE UNITED STATES

No. 09–893

AT&T MOBILITY LLC, PETITIONER *v.* VINCENT CONCEPCION ET UX.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

[April 27, 2011]

JUSTICE SCALIA delivered the opinion of the Court.

Section 2 of the Federal Arbitration Act (FAA) makes agreements to arbitrate "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U. S. C. §2. We consider whether the FAA prohibits States from conditioning the enforceability of certain arbitration agreements on the availability of classwide arbitration procedures.

I

In February 2002, Vincent and Liza Concepcion entered into an agreement for the sale and servicing of cellular telephones with AT&T Mobility LCC (AT&T).[1] The contract provided for arbitration of all disputes between the parties, but required that claims be brought in the parties' "individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding." App.

[1]The Conceptions' original contract was with Cingular Wireless. AT&T acquired Cingular in 2005 and renamed the company AT&T Mobility in 2007. *Laster* v. *AT&T Mobility LLC*, 584 F. 3d 849, 852, n. 1 (CA9 2009).

to Pet. for Cert 61a.[2] The agreement authorized AT&T to make unilateral amendments, which it did to the arbitration provision on several occasions. The version at issue in this case reflects revisions made in December 2006, which the parties agree are controlling.

The revised agreement provides that customers may initiate dispute proceedings by completing a one-page Notice of Dispute form available on AT&T's Web site. AT&T may then offer to settle the claim; if it does not, or if the dispute is not resolved within 30 days, the customer may invoke arbitration by filing a separate Demand for Arbitration, also available on AT&T's Web site. In the event the parties proceed to arbitration, the agreement specifies that AT&T must pay all costs for nonfrivolous claims; that arbitration must take place in the county in which the customer is billed; that, for claims of $10,000 or less, the customer may choose whether the arbitration proceeds in person, by telephone, or based only on submissions; that either party may bring a claim in small claims court in lieu of arbitration; and that the arbitrator may award any form of individual relief, including injunctions and presumably punitive damages. The agreement, moreover, denies AT&T any ability to seek reimbursement of its attorney's fees, and, in the event that a customer receives an arbitration award greater than AT&T's last written settlement offer, requires AT&T to pay a $7,500 minimum recovery and twice the amount of the claimant's attorney's fees.[3]

The Concepcions purchased AT&T service, which was advertised as including the provision of free phones; they

---

[2] That provision further states that "the arbitrator may not consolidate more than one person's claims, and may not otherwise preside over any form of a representative or class proceeding." App. to Pet. for Cert. 61a.

[3] The guaranteed minimum recovery was increased in 2009 to $10,000. Brief for Petitioner 7.

were not charged for the phones, but they were charged $30.22 in sales tax based on the phones' retail value. In March 2006, the Concepcions filed a complaint against AT&T in the United States District Court for the Southern District of California. The complaint was later consolidated with a putative class action alleging, among other things, that AT&T had engaged in false advertising and fraud by charging sales tax on phones it advertised as free.

In March 2008, AT&T moved to compel arbitration under the terms of its contract with the Concepcions. The Concepcions opposed the motion, contending that the arbitration agreement was unconscionable and unlawfully exculpatory under California law because it disallowed classwide procedures. The District Court denied AT&T's motion. It described AT&T's arbitration agreement favorably, noting, for example, that the informal dispute-resolution process was "quick, easy to use" and likely to "promp[t] full or . . . even excess payment to the customer *without* the need to arbitrate or litigate"; that the $7,500 premium functioned as "a substantial inducement for the consumer to pursue the claim in arbitration" if a dispute was not resolved informally; and that consumers who were members of a class would likely be worse off. *Laster* v. *T-Mobile USA, Inc.*, 2008 WL 5216255, *11–*12 (SD Cal., Aug. 11, 2008). Nevertheless, relying on the California Supreme Court's decision in *Discover Bank* v. *Superior Court*, 36 Cal. 4th 148, 113 P. 3d 1100 (2005), the court found that the arbitration provision was unconscionable because AT&T had not shown that bilateral arbitration adequately substituted for the deterrent effects of class actions. *Laster*, 2008 WL 5216255, *14.

The Ninth Circuit affirmed, also finding the provision unconscionable under California law as announced in *Discover Bank*. *Laster* v. *AT&T Mobility LLC*, 584 F. 3d 849, 855 (2009). It also held that the *Discover Bank* rule was not preempted by the FAA because that rule was

simply "a refinement of the unconscionability analysis applicable to contracts generally in California." 584 F. 3d, at 857. In response to AT&T's argument that the Concepcions' interpretation of California law discriminated against arbitration, the Ninth Circuit rejected the contention that "'class proceedings will reduce the efficiency and expeditiousness of arbitration'" and noted that "'*Discover Bank* placed arbitration agreements with class action waivers on the *exact same footing* as contracts that bar class action litigation outside the context of arbitration.'" *Id.*, at 858 (quoting *Shroyer* v. *New Cingular Wireless Services, Inc.*, 498 F. 3d 976, 990 (CA9 2007)).

We granted certiorari, 560 U. S. ___ (2010).

II

The FAA was enacted in 1925 in response to widespread judicial hostility to arbitration agreements. See *Hall Street Associates, L. L. C.* v. *Mattel, Inc.*, 552 U. S. 576, 581 (2008). Section 2, the "primary substantive provision of the Act," *Moses H. Cone Memorial Hospital* v. *Mercury Constr. Corp.*, 460 U. S. 1, 24 (1983), provides, in relevant part, as follows:

> "A written provision in any maritime transaction or a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U. S. C. §2.

We have described this provision as reflecting both a "liberal federal policy favoring arbitration," *Moses H. Cone*, *supra,* at 24, and the "fundamental principle that arbitration is a matter of contract," *Rent-A-Center, West, Inc.* v. *Jackson*, 561 U. S. ____ , ____ (2010) (slip op., at 3). In line with these principles, courts must place arbitration

agreements on an equal footing with other contracts, *Buckeye Check Cashing, Inc.* v. *Cardegna*, 546 U. S. 440, 443 (2006), and enforce them according to their terms, *Volt Information Sciences, Inc.* v. *Board of Trustees of Leland Stanford Junior Univ.*, 489 U. S. 468, 478 (1989).

The final phrase of §2, however, permits arbitration agreements to be declared unenforceable "upon such grounds as exist at law or in equity for the revocation of any contract." This saving clause permits agreements to arbitrate to be invalidated by "generally applicable contract defenses, such as fraud, duress, or unconscionability," but not by defenses that apply only to arbitration or that derive their meaning from the fact that an agreement to arbitrate is at issue. *Doctor's Associates*, *Inc.* v. *Casarotto*, 517 U. S. 681, 687 (1996); see also *Perry* v. *Thomas*, 482 U. S. 483, 492–493, n. 9 (1987). The question in this case is whether §2 preempts California's rule classifying most collective-arbitration waivers in consumer contracts as unconscionable. We refer to this rule as the *Discover Bank* rule.

Under California law, courts may refuse to enforce any contract found "to have been unconscionable at the time it was made," or may "limit the application of any unconscionable clause." Cal. Civ. Code Ann. §1670.5(a) (West 1985). A finding of unconscionability requires "a 'procedural' and a 'substantive' element, the former focusing on 'oppression' or 'surprise' due to unequal bargaining power, the latter on 'overly harsh' or 'one-sided' results." *Armendariz* v. *Foundation Health Pyschcare Servs., Inc.*, 24 Cal. 4th 83, 114, 6 P. 3d 669, 690 (2000); accord, *Discover Bank*, 36 Cal. 4th, at 159–161, 113 P. 3d, at 1108.

In *Discover Bank*, the California Supreme Court applied this framework to class-action waivers in arbitration agreements and held as follows:

"[W]hen the waiver is found in a consumer contract of

> adhesion in a setting in which disputes between the contracting parties predictably involve small amounts of damages, and when it is alleged that the party with the superior bargaining power has carried out a scheme to deliberately cheat large numbers of consumers out of individually small sums of money, then . . . the waiver becomes in practice the exemption of the party 'from responsibility for [its] own fraud, or willful injury to the person or property of another.' Under these circumstances, such waivers are unconscionable under California law and should not be enforced." *Id.*, at 162, 113 P. 3d, at 1110 (quoting Cal. Civ. Code Ann. §1668).

California courts have frequently applied this rule to find arbitration agreements unconscionable. See, *e.g.*, *Cohen* v. *DirecTV, Inc.*, 142 Cal. App. 4th 1442, 1451–1453, 48 Cal. Rptr. 3d 813, 819–821 (2006); *Klussman* v. *Cross Country Bank*, 134 Cal. App. 4th 1283, 1297, 36 Cal Rptr. 3d 728, 738–739 (2005); *Aral* v. *EarthLink, Inc.*, 134 Cal. App. 4th 544, 556–557, 36 Cal. Rptr. 3d 229, 237–239 (2005).

III

A

The Concepcions argue that the *Discover Bank* rule, given its origins in California's unconscionability doctrine and California's policy against exculpation, is a ground that "exist[s] at law or in equity for the revocation of any contract" under FAA §2. Moreover, they argue that even if we construe the *Discover Bank* rule as a prohibition on collective-action waivers rather than simply an application of unconscionability, the rule would still be applicable to all dispute-resolution contracts, since California prohibits waivers of class litigation as well. See *America Online, Inc.* v. *Superior Ct.*, 90 Cal. App. 4th 1, 17–18, 108 Cal. Rptr. 2d 699, 711–713 (2001).

When state law prohibits outright the arbitration of a

particular type of claim, the analysis is straightforward: The conflicting rule is displaced by the FAA. *Preston* v. *Ferrer*, 552 U. S. 346, 353 (2008). But the inquiry becomes more complex when a doctrine normally thought to be generally applicable, such as duress or, as relevant here, unconscionability, is alleged to have been applied in a fashion that disfavors arbitration. In *Perry* v. *Thomas*, 482 U. S. 483 (1987), for example, we noted that the FAA's preemptive effect might extend even to grounds traditionally thought to exist "'at law or in equity for the revocation of any contract.'" *Id.*, at 492, n. 9 (emphasis deleted). We said that a court may not "rely on the uniqueness of an agreement to arbitrate as a basis for a state-law holding that enforcement would be unconscionable, for this would enable the court to effect what . . . the state legislature cannot." *Id.*, at 493, n. 9.

An obvious illustration of this point would be a case finding unconscionable or unenforceable as against public policy consumer arbitration agreements that fail to provide for judicially monitored discovery. The rationalizations for such a holding are neither difficult to imagine nor different in kind from those articulated in *Discover Bank*. A court might reason that no consumer would knowingly waive his right to full discovery, as this would enable companies to hide their wrongdoing. Or the court might simply say that such agreements are exculpatory—restricting discovery would be of greater benefit to the company than the consumer, since the former is more likely to be sued than to sue. See *Discover Bank*, *supra*, at 161, 113 P. 3d, at 1109 (arguing that class waivers are similarly one-sided). And, the reasoning would continue, because such a rule applies the general principle of unconscionability or public-policy disapproval of exculpatory agreements, it is applicable to "any" contract and thus preserved by §2 of the FAA. In practice, of course, the rule would have a disproportionate impact on arbitration

agreements; but it would presumably apply to contracts purporting to restrict discovery in litigation as well.

Other examples are easy to imagine. The same argument might apply to a rule classifying as unconscionable arbitration agreements that fail to abide by the Federal Rules of Evidence, or that disallow an ultimate disposition by a jury (perhaps termed "a panel of twelve lay arbitrators" to help avoid preemption). Such examples are not fanciful, since the judicial hostility towards arbitration that prompted the FAA had manifested itself in "a great variety" of "devices and formulas" declaring arbitration against public policy. *Robert Lawrence Co.* v. *Devonshire Fabrics, Inc.*, 271 F. 2d 402, 406 (CA2 1959). And although these statistics are not definitive, it is worth noting that California's courts have been more likely to hold contracts to arbitrate unconscionable than other contracts. Broome, An Unconscionable Applicable of the Unconscionability Doctrine: How the California Courts are Circumventing the Federal Arbitration Act, 3 Hastings Bus. L. J. 39, 54, 66 (2006); Randall, Judicial Attitudes Toward Arbitration and the Resurgence of Unconscionability, 52 Buffalo L. Rev. 185, 186–187 (2004).

The Concepcions suggest that all this is just a parade of horribles, and no genuine worry. "Rules aimed at destroying arbitration" or "demanding procedures incompatible with arbitration," they concede, "would be preempted by the FAA because they cannot sensibly be reconciled with Section 2." Brief for Respondents 32. The "grounds" available under §2's saving clause, they admit, "should not be construed to include a State's mere preference for procedures that are incompatible with arbitration and 'would wholly eviscerate arbitration agreements.'" *Id.*, at 33 (quoting *Carter* v. *SSC Odin Operating Co., LLC*, 237 Ill. 2d 30, 50, 927 N. E. 2d 1207, 1220 (2010)).[4]

---

[4]The dissent seeks to fight off even this eminently reasonable conces-

We largely agree. Although §2's saving clause preserves generally applicable contract defenses, nothing in it suggests an intent to preserve state-law rules that stand as an obstacle to the accomplishment of the FAA's objectives. Cf. *Geier* v. *American Honda Motor Co.*, 529 U. S. 861, 872 (2000); *Crosby* v. *National Foreign Trade Council*, 530 U. S. 363, 372–373 (2000). As we have said, a federal statute's saving clause "'cannot in reason be construed as [allowing] a common law right, the continued existence of which would be absolutely inconsistent with the provisions of the act. In other words, the act cannot be held to destroy itself.'" *American Telephone & Telegraph Co.* v. *Central Office Telephone, Inc.*, 524 U. S. 214, 227–228 (1998) (quoting *Texas & Pacific R. Co.* v. *Abilene Cotton Oil Co.*, 204 U. S. 426, 446 (1907)).

We differ with the Concepcions only in the application of this analysis to the matter before us. We do not agree that rules requiring judicially monitored discovery or adherence to the Federal Rules of Evidence are "a far cry from this case." Brief for Respondents 32. The overarching purpose of the FAA, evident in the text of §§2, 3, and 4, is to ensure the enforcement of arbitration agreements according to their terms so as to facilitate streamlined proceedings. Requiring the availability of classwide arbitration interferes with fundamental attributes of arbitration and thus creates a scheme inconsistent with the FAA.

B

The "principal purpose" of the FAA is to "ensur[e] that private arbitration agreements are enforced according to

---

sion. It says that to its knowledge "we have not . . . applied the Act to strike down a state statute that treats arbitrations on par with judicial and administrative proceedings," *post*, at 10 (opinion of BREYER, J.), and that "we should think more than twice before invalidating a state law that . . . puts agreements to arbitrate and agreements to litigate 'upon the same footing'" *post*, at 4–5.

their terms." *Volt*, 489 U. S., at 478; see also *Stolt-Nielsen S. A.* v. *AnimalFeeds Int'l Corp.*, 559 U. S. ___, ___ (2010) (slip op., at 17). This purpose is readily apparent from the FAA's text. Section 2 makes arbitration agreements "valid, irrevocable, and enforceable" as written (subject, of course, to the saving clause); §3 requires courts to stay litigation of arbitral claims pending arbitration of those claims "in accordance with the terms of the agreement"; and §4 requires courts to compel arbitration "in accordance with the terms of the agreement" upon the motion of either party to the agreement (assuming that the "making of the arbitration agreement or the failure . . . to perform the same" is not at issue). In light of these provisions, we have held that parties may agree to limit the issues subject to arbitration, *Mitsubishi Motors Corp.* v. *Soler Chrysler-Plymouth, Inc.*, 473 U. S. 614, 628 (1985), to arbitrate according to specific rules, *Volt*, *supra,* at 479, and to limit *with whom* a party will arbitrate its disputes, *Stolt-Nielsen*, *supra,* at ___ (slip op., at 19).

The point of affording parties discretion in designing arbitration processes is to allow for efficient, streamlined procedures tailored to the type of dispute. It can be specified, for example, that the decisionmaker be a specialist in the relevant field, or that proceedings be kept confidential to protect trade secrets. And the informality of arbitral proceedings is itself desirable, reducing the cost and increasing the speed of dispute resolution. *14 Penn Plaza LLC* v. *Pyett*, 556 U. S. ___, ___ (2009) (slip op., at 20); *Mitsubishi Motors Corp.*, *supra,* at 628.

The dissent quotes *Dean Witter Reynolds Inc.* v. *Byrd*, 470 U. S. 213, 219 (1985), as "'reject[ing] the suggestion that the overriding goal of the Arbitration Act was to promote the expeditious resolution of claims.'" *Post*, at 4 (opinion of BREYER, J.). That is greatly misleading. After saying (accurately enough) that "the overriding goal of the Arbitration Act was [not] to promote the expeditious reso-

lution of claims," but to "ensure judicial enforcement of privately made agreements to arbitrate," 470 U. S., at 219, *Dean Witter* went on to explain: "This is not to say that Congress was blind to the potential benefit of the legislation for expedited resolution of disputes. Far from it . . . ." *Id.*, at 220. It then quotes a House Report saying that "the costliness and delays of litigation . . . can be largely eliminated by agreements for arbitration." *Ibid.* (quoting H. R. Rep. No. 96, 68th Cong., 1st Sess., 2 (1924)). The concluding paragraph of this part of its discussion begins as follows:

> "We therefore are not persuaded by the argument that the conflict between two goals of the Arbitration Act—enforcement of private agreements and encouragement of efficient and speedy dispute resolution—must be resolved in favor of the latter in order to realize the intent of the drafters." 470 U. S., at 221.

In the present case, of course, those "two goals" do not conflict—and it is the dissent's view that would frustrate *both* of them.

Contrary to the dissent's view, our cases place it beyond dispute that the FAA was designed to promote arbitration. They have repeatedly described the Act as "embod[ying] [a] national policy favoring arbitration," *Buckeye Check Cashing*, 546 U. S., at 443, and "a liberal federal policy favoring arbitration agreements, notwithstanding any state substantive or procedural policies to the contrary," *Moses H. Cone*, 460 U. S., at 24; see also *Hall Street Assocs.*, 552 U. S., at 581. Thus, in *Preston* v. *Ferrer*, holding preempted a state-law rule requiring exhaustion of administrative remedies before arbitration, we said: "A prime objective of an agreement to arbitrate is to achieve 'streamlined proceedings and expeditious results,'" which objective would be "frustrated" by requiring a dispute to be heard by an agency first. 552 U. S., at 357–358. That

rule, we said, would "at the least, hinder speedy resolution of the controversy." *Id.*, at 358.[5]

California's *Discover Bank* rule similarly interferes with arbitration. Although the rule does not *require* classwide arbitration, it allows any party to a consumer contract to demand it *ex post.* The rule is limited to adhesion contracts, *Discover Bank*, 36 Cal. 4th, at 162–163, 113 P. 3d, at 1110, but the times in which consumer contracts were anything other than adhesive are long past.[6] *Carbajal* v. *H&R Block Tax Servs., Inc.*, 372 F. 3d 903, 906 (CA7 2004); see also *Hill* v. *Gateway 2000, Inc.*, 105 F. 3d 1147, 1149 (CA7 1997). The rule also requires that damages be predictably small, and that the consumer allege a scheme to cheat consumers. *Discover Bank*, *supra,* at 162–163, 113 P. 3d, at 1110. The former requirement, however, is

---

[5] Relying upon nothing more indicative of congressional understanding than statements of witnesses in committee hearings and a press release of Secretary of Commerce Herbert Hoover, the dissent suggests that Congress "thought that arbitration would be used primarily where merchants sought to resolve disputes of fact . . . [and] possessed roughly equivalent bargaining power." *Post*, at 6. Such a limitation appears nowhere in the text of the FAA and has been explicitly rejected by our cases. "Relationships between securities dealers and investors, for example, may involve unequal bargaining power, but we [have] nevertheless held . . . that agreements to arbitrate in that context are enforceable." *Gilmer* v. *Interstate/Johnson Lane Corp.*, 500 U. S. 20, 33 (1991); see also *id.*, at 32–33 (allowing arbitration of claims arising under the Age Discrimination in Employment Act of 1967 despite allegations of unequal bargaining power between employers and employees). Of course the dissent's disquisition on legislative history fails to note that it contains nothing—not even the testimony of a stray witness in committee hearings—that contemplates the existence of class arbitration.

[6] Of course States remain free to take steps addressing the concerns that attend contracts of adhesion—for example, requiring class-action-waiver provisions in adhesive arbitration agreements to be highlighted. Such steps cannot, however, conflict with the FAA or frustrate its purpose to ensure that private arbitration agreements are enforced according to their terms.

toothless and malleable (the Ninth Circuit has held that damages of $4,000 are sufficiently small, see *Oestreicher* v. *Alienware Corp.*, 322 Fed. Appx. 489, 492 (2009) (unpublished)), and the latter has no limiting effect, as all that is required is an allegation. Consumers remain free to bring and resolve their disputes on a bilateral basis under *Discover Bank*, and some may well do so; but there is little incentive for lawyers to arbitrate on behalf of individuals when they may do so for a class and reap far higher fees in the process. And faced with inevitable class arbitration, companies would have less incentive to continue resolving potentially duplicative claims on an individual basis.

Although we have had little occasion to examine classwide arbitration, our decision in *Stolt-Nielsen* is instructive. In that case we held that an arbitration panel exceeded its power under §10(a)(4) of the FAA by imposing class procedures based on policy judgments rather than the arbitration agreement itself or some background principle of contract law that would affect its interpretation. 559 U. S., at ___ (slip op., at 20–23). We then held that the agreement at issue, which was silent on the question of class procedures, could not be interpreted to allow them because the "changes brought about by the shift from bilateral arbitration to class-action arbitration" are "fundamental." *Id.*, at ___ (slip op., at 22). This is obvious as a structural matter: Classwide arbitration includes absent parties, necessitating additional and different procedures and involving higher stakes. Confidentiality becomes more difficult. And while it is theoretically possible to select an arbitrator with some expertise relevant to the class-certification question, arbitrators are not generally knowledgeable in the often-dominant procedural aspects of certification, such as the protection of absent parties. The conclusion follows that class arbitration, to the extent it is manufactured by *Discover Bank* rather than consensual, is inconsistent with the FAA.

First, the switch from bilateral to class arbitration sacrifices the principal advantage of arbitration—its informality—and makes the process slower, more costly, and more likely to generate procedural morass than final judgment. "In bilateral arbitration, parties forgo the procedural rigor and appellate review of the courts in order to realize the benefits of private dispute resolution: lower costs, greater efficiency and speed, and the ability to choose expert adjudicators to resolve specialized disputes." 559 U. S., at ___ (slip op., at 21). But before an arbitrator may decide the merits of a claim in classwide procedures, he must first decide, for example, whether the class itself may be certified, whether the named parties are sufficiently representative and typical, and how discovery for the class should be conducted. A cursory comparison of bilateral and class arbitration illustrates the difference. According to the American Arbitration Association (AAA), the average consumer arbitration between January and August 2007 resulted in a disposition on the merits in six months, four months if the arbitration was conducted by documents only. AAA, Analysis of the AAA's Consumer Arbitration Caseload, online at http://www.adr.org/si.asp?id=5027 (all Internet materials as visited Apr. 25, 2011, and available in Clerk of Court's case file). As of September 2009, the AAA had opened 283 class arbitrations. Of those, 121 remained active, and 162 had been settled, withdrawn, or dismissed. Not a single one, however, had resulted in a final award on the merits. Brief for AAA as *Amicus Curiae* in *Stolt-Nielsen,* O. T. 2009, No. 08–1198, pp. 22–24. For those cases that were no longer active, the median time from filing to settlement, withdrawal, or dismissal—not judgment on the merits—was 583 days, and the mean was 630 days. *Id.*, at 24.[7]

---

[7]The dissent claims that class arbitration should be compared to class litigation, not bilateral arbitration. *Post*, at 6–7. Whether arbi-

Second, class arbitration *requires* procedural formality. The AAA's rules governing class arbitrations mimic the Federal Rules of Civil Procedure for class litigation. Compare AAA, Supplementary Rules for Class Arbitrations (effective Oct. 8, 2003), online at http://www.adr.org/sp.asp?id=21936, with Fed. Rule Civ. Proc. 23. And while parties can alter those procedures by contract, an alternative is not obvious. If procedures are too informal, absent class members would not be bound by the arbitration. For a class-action money judgment to bind absentees in litigation, class representatives must at all times adequately represent absent class members, and absent members must be afforded notice, an opportunity to be heard, and a right to opt out of the class. *Phillips Petroleum Co.* v. *Shutts*, 472 U. S. 797, 811–812 (1985). At least this amount of process would presumably be required for absent parties to be bound by the results of arbitration.

We find it unlikely that in passing the FAA Congress meant to leave the disposition of these procedural requirements to an arbitrator. Indeed, class arbitration was not even envisioned by Congress when it passed the FAA in 1925; as the California Supreme Court admitted in *Discover Bank*, class arbitration is a "relatively recent development." 36 Cal. 4th, at 163, 113 P. 3d, at 1110. And it is at the very least odd to think that an arbitrator would be entrusted with ensuring that third parties' due process rights are satisfied.

Third, class arbitration greatly increases risks to defendants. Informal procedures do of course have a cost: The absence of multilayered review makes it more likely that errors will go uncorrected. Defendants are willing to accept the costs of these errors in arbitration, since their

---

trating a class is more desirable than litigating one, however, is not relevant. A State cannot defend a rule requiring arbitration-by-jury by saying that parties will still prefer it to trial-by-jury.

impact is limited to the size of individual disputes, and presumably outweighed by savings from avoiding the courts. But when damages allegedly owed to tens of thousands of potential claimants are aggregated and decided at once, the risk of an error will often become unacceptable. Faced with even a small chance of a devastating loss, defendants will be pressured into settling questionable claims. Other courts have noted the risk of "in terrorem" settlements that class actions entail, see, *e.g.*, *Kohen* v. *Pacific Inv. Management Co. LLC*, 571 F. 3d 672, 677–678 (CA7 2009), and class arbitration would be no different.

Arbitration is poorly suited to the higher stakes of class litigation. In litigation, a defendant may appeal a certification decision on an interlocutory basis and, if unsuccessful, may appeal from a final judgment as well. Questions of law are reviewed *de novo* and questions of fact for clear error. In contrast, 9 U. S. C. §10 allows a court to vacate an arbitral award *only* where the award "was procured by corruption, fraud, or undue means"; "there was evident partiality or corruption in the arbitrators"; "the arbitrators were guilty of misconduct in refusing to postpone the hearing . . . or in refusing to hear evidence pertinent and material to the controversy[,] or of any other misbehavior by which the rights of any party have been prejudiced"; or if the "arbitrators exceeded their powers, or so imperfectly executed them that a mutual, final, and definite award . . . was not made." The AAA rules do authorize judicial review of certification decisions, but this review is unlikely to have much effect given these limitations; review under §10 focuses on misconduct rather than mistake. And parties may not contractually expand the grounds or nature of judicial review. *Hall Street Assocs.*, 552 U. S., at 578. We find it hard to believe that defendants would bet the company with no effective means of review, and even harder to believe that Congress would have intended to

allow state courts to force such a decision.[8]

The Concepcions contend that because parties may and sometimes do agree to aggregation, class procedures are not necessarily incompatible with arbitration. But the same could be said about procedures that the Concepcions admit States may not superimpose on arbitration: Parties *could* agree to arbitrate pursuant to the Federal Rules of Civil Procedure, or pursuant to a discovery process rivaling that in litigation. Arbitration is a matter of contract, and the FAA requires courts to honor parties' expectations. *Rent-A-Center*, *West*, 561 U. S., at ___ (slip op., at 3). But what the parties in the aforementioned examples would have agreed to is not arbitration as envisioned by the FAA, lacks its benefits, and therefore may not be required by state law.

The dissent claims that class proceedings are necessary to prosecute small-dollar claims that might otherwise slip through the legal system. See *post*, at 9. But States cannot require a procedure that is inconsistent with the FAA, even if it is desirable for unrelated reasons. Moreover, the claim here was most unlikely to go unresolved. As noted earlier, the arbitration agreement provides that AT&T will pay claimants a minimum of $7,500 and twice their attorney's fees if they obtain an arbitration award greater than AT&T's last settlement offer. The District Court

---

[8]The dissent cites three large arbitration awards (none of which stems from classwide arbitration) as evidence that parties are willing to submit large claims before an arbitrator. *Post*, at 7–8. Those examples might be in point if it could be established that the size of the arbitral dispute was predictable when the arbitration agreement was entered. Otherwise, all the cases prove is that arbitrators can give huge awards—which we have never doubted. The point is that in class-action arbitration huge awards (with limited judicial review) will be entirely predictable, thus rendering arbitration unattractive. It is not reasonably deniable that requiring consumer disputes to be arbitrated on a classwide basis will have a substantial deterrent effect on incentives to arbitrate.

found this scheme sufficient to provide incentive for the individual prosecution of meritorious claims that are not immediately settled, and the Ninth Circuit admitted that aggrieved customers who filed claims would be "essentially guarantee[d]" to be made whole, 584 F. 3d, at 856, n. 9. Indeed, the District Court concluded that the Concepcions were *better off* under their arbitration agreement with AT&T than they would have been as participants in a class action, which "could take months, if not years, and which may merely yield an opportunity to submit a claim for recovery of a small percentage of a few dollars." *Laster*, 2008 WL 5216255, at *12.

* * *

Because it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," *Hines* v. *Davidowitz*, 312 U. S. 52, 67 (1941), California's *Discover Bank* rule is preempted by the FAA. The judgment of the Ninth Circuit is reversed, and the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

Article 2A.
Identity Theft Protection Act.

§ 75-60. Title.

This Article shall be known and may be cited as the "Identity Theft Protection Act". (2005-414, s. 1.)

§ 75-61. Definitions.

The following definitions apply in this Article:

(1) "Business". – A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency.

(2) "Consumer". – An individual.

(3) "Consumer report" or "credit report". – Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for any of the following:

a. Credit to be used primarily for personal, family, or household purposes.

b. Employment purposes.

c. Any other purpose authorized under 15 U.S.C. § 168l(b).

(4) "Consumer reporting agency". – Any person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

(5) "Credit card". – Has the same meaning as in section 103 of the Truth in Lending Act (15 U.S.C. § 160, et seq.).

(6) "Debit card". – Any card or device issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account holding assets of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor, or services.

(7) "Disposal" includes the following:

a. The discarding or abandonment of records containing personal information.

b. The sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal information, or other nonpaper media upon which records of personal information are stored, or other equipment for nonpaper storage of information.

(8) "Encryption". – The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

(9) "Person". – Any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.

(10) "Personal information". – A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.

(11) "Proper identification". – Information generally deemed sufficient to identify a person. If a person is unable to reasonably identify himself or herself with the information described above, a consumer reporting agency may require additional information concerning the consumer's employment and personal or family history in order to verify the consumer's identity.

(12) "Records". – Any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(13) "Redaction". – The rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.

(14) "Security breach". – An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

(15) "Security freeze". – Notice placed in a credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer. (2005-414, s. 1.)

§ 75-62. Social security number protection.

(a) Except as provided in subsection (b) of this section, a business may not do any of the following:

(1) Intentionally communicate or otherwise make available to the general public an individual's social security number.

(2) Intentionally print or imbed an individual's social security number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification

number or other authentication device is also required to access the Internet Web site.

(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed.

(6) Sell, lease, loan, trade, rent, or otherwise intentionally disclose an individual's social security number to a third party without written consent to the disclosure from the individual, when the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's social security number.

(b) Subsection (a) of this section shall not apply in the following instances:

(1) When a social security number is included in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the social security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b)(2). A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(2) To the collection, use, or release of a social security number for internal verification or administrative purposes.

(3) To the opening of an account or the provision of or payment for a product or service authorized by an individual.

(4) To the collection, use, or release of a social security number to investigate or prevent fraud, conduct background checks, conduct social or scientific research, collect a debt, obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq., undertake a permissible purpose enumerated under Gramm Leach Bliley, 12 C.F.R. § 216.13-15, or locate an individual who is missing, a lost relative, or due a benefit, such as a pension, insurance, or unclaimed property benefit.

(5) To a business acting pursuant to a court order, warrant, subpoena, or when otherwise required by law.

(6) To a business providing the social security number to a federal, state, or local government entity, including a law enforcement agency, court, or their agents or assigns.

(7) To a social security number that has been redacted.

(c) A business covered by this section shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this Article are implemented.

(d) A violation of this section is a violation of G.S. 75-1.1. (2005-414, s. 1.)

§ 75-63. Security freeze.

(a) A consumer may place a security freeze on the consumer's credit report by making a request to a consumer reporting agency in accordance with this subsection. A security freeze shall prohibit, subject to exceptions in subsection (l) of this section, the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. When a security freeze is in place, a consumer reporting agency may not release the consumer's credit report or information to a third party without prior express authorization from the consumer. This subsection does not prevent a consumer

reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report, provided that the consumer reporting agency does not state or otherwise imply to the third party that the consumer's security freeze reflects a negative credit score, history, report, or rating. A consumer reporting agency shall place a security freeze on a consumer's credit report if the consumer requests a security freeze by any of the following methods:

(1) First-class mail.
(2) Telephone call.
(3) Secure Web site or secure electronic mail connection.

(a1) A nationwide consumer reporting agency, as defined in section 603(p) [15 U.S.C. § 1681a(p)] of the federal Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq., that receives a request from a consumer residing in this State to place a security freeze on the consumer's file, shall provide a notice communicating to the consumer that the freeze is only placed with the consumer reporting agency to which the consumer directed the request. The notice shall provide to the consumer the Web site, postal address, and telephone number of the other nationwide consumer reporting agencies and of the North Carolina Attorney General's Office and shall inform the consumer that he or she may use this information to contact other nationwide consumer reporting agencies to make security freeze requests and obtain information on combating identity theft. No part of the notice to the consumer shall be used to make a solicitation for other goods and services.

(b) A consumer reporting agency shall place a security freeze on a consumer's credit report no later than three business days after receiving a written request from the consumer by mail. A consumer reporting agency that receives such a request electronically or by telephone shall comply with the request within 24 hours of receiving the request.

(c) The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within three business days of placing the freeze and at the same time shall provide the consumer with a unique personal identification number or password, other than the consumer's social security number, to be used by the consumer when providing authorization for the release of the consumer's credit report for a specific period of time, or to a specific party, or for permanently lifting the freeze.

(d) If the consumer wishes to allow the consumer's credit report to be accessed for a specific period of time or by a specific party while a freeze is in place, the consumer shall contact the consumer reporting agency by mail, phone, or electronically, request that the freeze be lifted or lifted with respect to a specific party, and provide all of the following:

(1) Proper identification.
(2) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection (c) of this section.
(3) The proper information regarding the third party who is authorized to receive the consumer credit report or the time period for which the report shall be available to users of the credit report.

(e) Repealed by Session Laws 2009-355, s. 1, effective October 1, 2009.

(f) A consumer reporting agency that receives a request by mail from a consumer to lift a freeze on a credit report pursuant to subsection (d) of this section shall comply with the request no later than three business days after receiving the request. A consumer reporting agency that receives such a request electronically or by telephone shall comply with the request within 15 minutes of receiving the request.

(g) A consumer reporting agency shall remove, temporarily lift, or lift with respect to a specific third party a freeze placed on a consumer's credit report only in the following cases:

(1) Upon the consumer's request, pursuant to subsections (d) or (j) of this section.

(2) If the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a consumer reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this subdivision, the consumer reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(g1) A consumer reporting agency need not meet the time requirements provided in this section, only for such time as the occurrences prevent compliance, if any of the following occurrences apply:

(1) The consumer fails to meet the requirements of subsection (d) or (j) of this section.

(2) The consumer reporting agency's ability to remove, place, temporarily lift, or lift with respect to a specific party the security freeze is prevented by any of the following:

a. An act of God, including fire, earthquakes, hurricanes, storms, or similar natural disaster or phenomena.

b. Unauthorized or illegal acts by a third party, including terrorism, sabotage, riot, vandalism, labor strikes or disputes disrupting operations, or similar occurrences.

c. Operational interruption, including electrical failure, unanticipated delay in equipment or replacement part delivery, computer hardware or software failures inhibiting response time, or similar disruption.

d. Governmental action, including emergency orders or regulations, judicial or law enforcement action, or similar directives.

e. Regularly scheduled maintenance, during other than normal business hours, of, or updates to, the consumer reporting agency's systems.

f. Commercially reasonable maintenance of, or repair to, the consumer reporting agency's systems that is unexpected or unscheduled.

g. Receipt of a request outside of normal business hours.

(h) If a third party requests access to a consumer credit report on which a security freeze is in effect and this request is in connection with an application for credit or any other use and the consumer does not allow the consumer's credit report to be accessed for that specific period of time, the third party may treat the application as incomplete.

(i) If a consumer requests a security freeze pursuant to this section, the consumer reporting agency shall disclose to the consumer the process of placing and temporarily lifting a security freeze and the process for allowing access to information from the consumer's credit report for a specific period of time or to a specific third party while the security freeze is in place.

(j) A security freeze shall remain in place until the consumer requests that the security freeze be temporarily lifted for a specific period of time or to a specific third party or removed. A consumer reporting agency shall remove a security freeze within 15 minutes of receiving an electronic request for removal from the consumer or within three business days of receiving a written or telephonic request for removal from the consumer, who provides all of the following:

(1) Proper identification.

(2) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection (c) of this section.

(k) A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

(l) The provisions of this section do not apply to the use of a consumer credit report by any of the following:

(1) A person, or the person's subsidiary, affiliate, agent, subcontractor, or assignee with whom the consumer has, or prior to assignment had, an

account, contract, or debtor-creditor relationship for the purposes of reviewing the active account or collecting the financial obligation owing for the account, contract, or debt.

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subsection (d) of this section for purposes of facilitating the extension of credit or other permissible use.

(3) Any person acting pursuant to a court order, warrant, or subpoena.

(4) A state or local agency, or its agents or assigns, which administers a program for establishing and enforcing child support obligations.

(5) A state or local agency, or its agents or assigns, acting to investigate fraud, including Medicaid fraud, or acting to investigate or collect delinquent taxes or assessments, including interest and penalties, unpaid court orders, or to fulfill any of its other statutory responsibilities.

(6) A federal, state, or local governmental entity, including law enforcement agency, court, or their agent or assigns.

(7) A person for the purposes of prescreening as defined by the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.

(8) Any person for the sole purpose of providing for a credit file monitoring subscription service to which the consumer has subscribed.

(9) A consumer reporting agency for the purpose of providing a consumer with a copy of the consumer's credit report upon the consumer's request.

(10) Any depository financial institution for checking, savings, and investment accounts.

(11) Any property and casualty insurance company for use in setting or adjusting a rate, adjusting a claim, or underwriting for property and casualty insurance purposes.

(12) A person for the purpose of furnishing or using credit reports for employment purposes pursuant to 15 U.S.C. § 1681b(b) or tenant screening pursuant to 15 U.S.C. § 1681b(a)(3)(F).

(13) A person for the purpose of criminal background record information.

(m) If a security freeze is in place, a consumer reporting agency shall not change any of the following official information in a credit report without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer's file: name, date of birth, social security number, and address. Written confirmation is not required for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and the former address.

(n) The following persons are not required to place in a credit report a security freeze pursuant to this section provided, however, that any person that is not required to place a security freeze on a credit report under the provisions of subdivision (3) of this subsection shall be subject to any security freeze placed on a credit report by another consumer reporting agency from which it obtains information:

(1) A check services or fraud prevention services company, which reports on incidents of fraud or issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers, or similar methods of payment.

(2) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or other similar negative information regarding a consumer to inquiring

banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution.

(3) A consumer reporting agency that does all of the following:

a. Acts only to resell credit information by assembling and merging information contained in a database of one or more credit reporting agencies.

b. Does not maintain a permanent database of credit information from which new credit reports are produced.

(o) A consumer reporting agency shall not charge a fee to put a security freeze in place, remove a freeze, or lift a freeze pursuant to subsection (d) or (j) of this section, provided that any such request is made electronically. If a request to put a security freeze in place is made by telephone or by mail, a consumer reporting agency may charge a fee to a consumer not to exceed three dollars ($3.00), except that a consumer reporting agency may not charge any fee to a consumer over the age of 62, to a victim of identity theft who has submitted a copy of a valid investigative or incident report or complaint with a law enforcement agency about the unlawful use of the victim's identifying information by another person, or to the victim's spouse. A consumer reporting agency shall not charge an additional fee to a consumer who requests to temporarily lift for a specific period of time or to a specific third party, reinstate, or remove a security freeze. A consumer reporting agency shall not charge a consumer for a onetime reissue of a replacement personal identification number. A consumer reporting agency may charge a fee not to exceed three dollars ($3.00) to provide any subsequent replacement personal identification number.

(o1) A parent or guardian of a minor residing in this State may, upon appropriate proof of identity and proof of their relationship to the minor, inquire of a nationwide consumer reporting agency, as defined in section 603(p) [15 U.S.C. § 1681a(p)] of the federal Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq., as to the existence of a credit report for the minor of the parent or guardian. If a credit report for the minor exists, the nationwide consumer reporting agency shall make reasonable efforts to prevent providing a credit report on the minor until the minor reaches the age of majority. If a credit report for the minor does not exist, the nationwide consumer reporting agency has no obligation to create one.

(p) At any time that a consumer is required to receive a summary of rights required under section 609 of the federal Fair Credit Reporting Act, the following notice shall be included:

"North Carolina Consumers Have the Right to Obtain a Security Freeze.

You have a right to place a "security freeze" on your credit report pursuant to North Carolina law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization. A security freeze can be requested in writing by first-class mail, by telephone, or electronically. You also may request a freeze by visiting the following Web site: [URL] or calling the following telephone number: [NUMBER].

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gains access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, rental housing, employment, investment, license, cellular phone, utilities, digital signature, Internet credit card transactions, or other services, including an extension of credit at point of sale.

The freeze will be placed within three business days if you request it by mail, or within 24 hours if you request it by telephone or electronically. When you place a security freeze on your credit report, within three business days, you will be sent a personal identification number or a

password to use when you want to remove the security freeze, temporarily lift it, or lift it with respect to a particular third party.

A freeze does not apply when you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control, or similar activities.

You should plan ahead and lift a freeze if you are actively seeking credit or services as a security freeze may slow your applications, as mentioned above.

You can remove a freeze, temporarily lift a freeze, or lift a freeze with respect to a particular third party by contacting the consumer reporting agency and providing all of the following:

(1) Your personal identification number or password,
(2) Proper identification to verify your identity, and
(3) Proper information regarding the period of time you want your report available to users of the credit report, or the third party with respect to which you want to lift the freeze.

A consumer reporting agency that receives a request from you to temporarily lift a freeze or to lift a freeze with respect to a particular third party on a credit report shall comply with the request no later than three business days after receiving the request by mail and no later than 15 minutes after receiving a request by telephone or electronically. A consumer reporting agency may charge you up to three dollars ($3.00) to institute a freeze if your request is made by telephone or by mail. A consumer reporting agency may not charge you any amount to freeze, remove a freeze, temporarily lift a freeze, or lift a freeze with respect to a particular third party, if any of the following are true:

(1) Your request is made electronically.
(2) You are over the age of 62.
(3) You are the victim of identity theft and have submitted a copy of a valid investigative or incident report or complaint with a law enforcement agency about the unlawful use of your identifying information by another person, or you are the spouse of such a person.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report."

(q) A violation of this section is a violation of G.S. 75-1.1. (2005-414, s. 1; 2006-158, s. 1; 2009-355, s. 1; 2009-550, s. 5.)

§ 75-64. Destruction of personal information records.

(a) Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.

(b) The reasonable measures must include:

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed.
(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed.
(3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.

(c) A business may, after due diligence, enter into a written contract with, and monitor compliance by, another party engaged in the business of record destruction to destroy personal information in a manner consistent with this section. Due diligence should ordinarily include one or more of the following:

(1) Reviewing an independent audit of the disposal business's operations or its compliance with this statute or its equivalent.

(2) Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review.

(3) Reviewing and evaluating the disposal business's information security policies or procedures or taking other appropriate measures to determine the competency and integrity of the disposal business.

(d) A disposal business that conducts business in North Carolina or disposes of personal information of residents of North Carolina must take all reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of personal information during or after the collection and transportation and disposing of such information.

(e) This section does not apply to any of the following:

(1) Any bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm Leach Bliley Act, 15 U.S.C. § 6801, et seq., as amended.

(2) Any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.

(3) Any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act, 15 U.S.C. § 1681, et seq., as amended.

(f) A violation of this section is a violation of G.S. 75-1.1, but any damages assessed against a business because of the acts or omissions of its nonmanagerial employees shall not be trebled as provided in G.S. 75-16 unless the business was negligent in the training, supervision, or monitoring of those employees. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation. (2005-414, s. 1.)

§ 75-65. Protection from security breaches.

(a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any

business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

(c) The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

(d) The notice shall be clear and conspicuous. The notice shall include all of the following:

(1) A description of the incident in general terms.

(2) A description of the type of personal information that was subject to the unauthorized access and acquisition.

(3) A description of the general acts of the business to protect the personal information from further unauthorized access.

(4) A telephone number for the business that the person may call for further information and assistance, if one exists.

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(6) The toll-free numbers and addresses for the major consumer reporting agencies.

(7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.

(3) Telephonic notice provided that contact is made directly with the affected persons.

(4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

a. E-mail notice when the business has an electronic mail address for the subject persons.

b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.

c. Notification to major statewide media.

(e1) In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

(g) Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable.

(h) A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration; and any revisions, additions, or substitutions relating to any of the said interagency guidance, shall be deemed to be in compliance with this section.

(i) A violation of this section is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

(j) Causes of action arising under this Article may not be assigned. (2005-414, s. 1; 2009-355, s. 2; 2009-573, s. 10.)

§ 75-66. Publication of personal information.

(a) It shall be a violation of this section for any person to knowingly broadcast or publish to the public on radio, television, cable television, in a writing of any kind, or on the Internet, the personal information of another with actual knowledge that the person whose personal information is disclosed has previously objected to any such disclosure.

(b) As used in this section, "person" means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity, but does not include any:

(1) Government, government subdivision or agency.

(2) Entity subject to federal requirements pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

(c) As used in this section, the phrase "personal information" includes a person's first name or first initial and last name in combination with any of the following information:

(1) Social security or employer taxpayer identification numbers.

(2) Drivers license, State identification card, or passport numbers.

(3) Checking account numbers.

(4) Savings account numbers.

(5) Credit card numbers.

(6) Debit card numbers.

(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).

(8) Digital signatures.

(9) Any other numbers or information that can be used to access a person's financial resources.
(10) Biometric data.
(11) Fingerprints.
(12) Passwords.

(d) Nothing in this section shall:
(1) Limit the requirements or obligations under any other section of this Article, including, but not limited to, G.S. 75-62 and G.S. 75-65.
(2) Apply to the collection, use, or release of personal information for a purpose permitted, authorized, or required by any federal, State, or local law, regulation, or ordinance.
(3) Apply to data integration efforts to implement the State's business intelligence strategy as provided by law or under contract.

(e) Any person whose property or person is injured by reason of a violation of this section may sue for civil damages pursuant to the provisions of G.S. 1-539.2C. (2007-534, s. 2; 2012-142, s. 6A.7A(h).)

§ 75-67. Reserved for future codification purposes.

§ 75-68. Reserved for future codification purposes.

§ 75-69. Reserved for future codification purposes.

§ 75-70. Reserved for future codification purposes.

§ 75-71. Reserved for future codification purposes.

§ 75-72. Reserved for future codification purposes.

§ 75-73. Reserved for future codification purposes.

§ 75-74. Reserved for future codification purposes.

§ 75-75. Reserved for future codification purposes.

§ 75-76. Reserved for future codification purposes.

§ 75-77. Reserved for future codification purposes.

§ 75-78. Reserved for future codification purposes.

§ 75-79. Reserved for future codification purposes.