APPENDIX 1 – VFS GLOBAL INCIDENT RESPONSE TEAM *(follow this template when forming Regional or Local Response Teams)*

IRT Leaders:

Team Function	Office/Title	Name	Phone	Email
Team Leader	Global CIO & VP Operational Excellence	AS (Brussels)	INFO REMOVED FOR CONFIDENTIALITY	
Risk	SVP Chief Risk Officer	PS (Greensboro)		
Legal	SVP General Counsel	AM (Greensboro)		

Additional Team members (internal) – appointed by IRT Leaders as required:

Team Function	Office/Title	Name	Phone	Email
Communications	VP Global Corporate Communications	Allison Long (Greensboro)		
HR	SVP Human Resources	Troy Heflin (Greensboro)		
Compliance	Global Director of Compliance	Estelle Skopan (Tokyo)		
InfoSec	Information Security Officer	Scott Toth (Greensboro)		
ITS	*To be designated by CIO*			
Operational Control	*to be designated by SVP Risk*			
Business Control	VP Global Controller	Jim Dwane (Greensboro)		

Additional Team members (external) – appointed/engaged by IRT Leaders as required:

Team Function	Appointed by	Name & Company	Phone	Email
Forensic examiners	Team Leader	nGuard		
PR Agency	Communications			
External Counsel	Legal	Name, Sheppard Mullin (Chicago & London)		
Law Enforcement	Team Leader & Legal	FBI Supervisory Special Agent – Cyber Division (location)		
Regulatory Authority (Banking and/or Data Privacy)	Legal & Compliance			
ID Theft protection or Others as required	Team Leader			

APPENDIX 2 – First Responder Tasks & Responsibilities:

Every Data Incident is different and may require different actions depending on the circumstances and the jurisdiction in which it occurs – check with your local VFS lawyer. Unless shorter response times are required by local law, we suggest an initial 30-day timeline for the fundamental steps which should be addressed when a Data Incident is suspected:

Time Frame (measured in days from notification of the Incident)	Task	Team Function(s) Responsible
Day of internal notification of Incident to Global IRT (Day 0)	Report suspected incident and notify Global Incident Response Team	*This will come from preferably within the Business by whoever first discovers or suspects a Data Incident.*
within Week 1	Identify likely source/cause of Data Incident	Team Leader & ITS (following receipt of Incident Report or other notification)
within Week 1	Confirm whether Personal Data has or may have been compromised and, if so, inform IRT Legal and InfoSec	Team Leader
within Week 1	Confirm whether employee Personal Data has or may have been compromised and, if so, inform IRT Legal & IRT HR	Team Leader
within Week 1	Confirm whether commercially sensitive business information/trade secrets has or may have been compromised and, if so, inform IRT Legal & IRT Risk	Team Leader
within Week 2	Determine extent or nature of Personal Data compromised and inform IRT Legal Team Leader (CIO/DPO)	ITS & InfoSec
within Week 2	Determine extent or nature of business information/trade secrets compromised and inform IRT Legal & IRT Risk	ITS & InfoSec
within Week 2	Initial containment steps such as isolating networks, disabling access, or remote wiping equipment, etc. should be taken where applicable.	ITS
within Weeks 2-3	Determine whether or not affected parties require to be notified (and whether any dealer notification is desired)	IRT Legal
within Weeks 2-3	Determine whether or not those affected will be notified anyway. If yes, Team Leader to liaise internally to obtain name & address file and pass to IRT Legal.	IRT Legal & Team Leader
within Weeks 2-3	Determine whether or not Law Enforcement need to be notified	IRT Leaders based on information & recommendation from InfoSec
within Weeks 2-3	Determine whether or not Regulatory Authorities need to be notified (Banking and/or Data Protection)	IRT Compliance & Team Leader (CIO/DPO)
Day 21	Executive Summary report to President	Team Leader
within Week 4	**Decision**: do we need/wish to offer ID Theft/Credit Monitoring services	IRT Leaders, CIO/DPO (if not already included) & President
within Week 4	**Decision**: scalability - can we handle in house or do we need call center/notification help	Team Leader & InfoSec & IRT Legal (& President – depending on scale)
within Week 4	Inform Communications of agreed action plan	Team Leader
within Week 4 (if required)	Prepare initial statement for press	IRT Communications (with advice from IRT Legal)
within Week 4 (if required)	Prepare Q&A for press enquiries	IRT Communications (with advice from IRT Legal)
within Week 4	Prepare Q&A for enquiries by affected parties and share with all Incident Response Team members. Team members should cascade further into their organizations as needed.	IRT Communications (with advice from IRT Legal)
Day 30 (if required)	Issue required or desired notifications	IRT Legal
By Day 30 - Only if deemed necessary/desirable	Issue press statement	IRT Communications
Day 30+ - only if deemed necessary/desirable	Start monitoring social media (issue statements/comments as needed)	IRT Communications